Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2010

Pedro Alexandre Sousa Gonçalves

Gestão de Qualidade de Serviço Baseada em Políticas

Universidade de Aveiro
2010
Departamento de Electrónica, Telecomunicações e Informática

Pedro Alexandre Sousa Gonçalves

Gestão de Qualidade de Serviço Baseada em Políticas

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Informática, realizada sob a orientação científica do Doutor José Luís Guimarães Oliveira, Professor Associado do Departamento de Electrónica Telecomunicações e Informática da Universidade de Aveiro, e do Doutor Rui Luís Andrade de Aguiar, Professor Associado do Departamento de Electrónica Telecomunicações e Informática da Universidade de Aveiro

Ao Rui e ao André

o júri
presidente

Professor Doutor Artur Manuel Soares da Silva
professor catedrático da Universidade de Aveiro

Professor Doutor Fernando Pedro Lopes Boavida Fernandes
professor catedrático da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Professor Doutor Joaquim Arnaldo Carvalho Martins
professor catedrático da Universidade de Aveiro

Professor Doutor Alexandre Júlio Teixeira Santos
professor associado da Escola de Engenharia da Universidade do Minho

Professor Doutor José Luís Guimarães Oliveira
professor associado da Universidade de Aveiro

Professor Doutor Rui Andrade de Aguiar
professor associado da Universidade de Aveiro

agradecimentos

A dimensão de um trabalho de doutoramento requer ao candidato disponibilidade e dedicação durante um longo período, especialmente quando este é levado a cabo em paralelo com o desenvolvimento de uma actividade profissional, só sendo possível com a colaboração científica, profissional e pessoal das pessoas próximas.

Agradeço em primeiro lugar ao meu orientador científico, Professor José Luís Oliveira, pelo seu rigor científico, sentido crítico e acompanhamento atento que enriqueceu e ajudou a completar este trabalho. Agradeço-lhe ainda pela sua enorme disponibilidade, pelo seu encorajamento e pela boa disposição que tornaram possível este trabalho, e fizeram crescer um imenso respeito e uma nova amizade.

Ao Professor Rui Aguiar, meu orientador científico, agradeço-lhe a opinião informada e o enorme sentido crítico que muitas vezes fizeram a diferença em momentos de escolha do melhor caminho, evitando trabalho inglório. Agradeço-lhe ainda o apoio e a disponibilização de recursos, especialmente para a participação em conferências.

À minha esposa devo agradecer-lhe a paciência e compreensão, bem como a disponibilidade de ler e comentar um extenso documento técnico.

Agradeço ao Instituto de Telecomunicações, minha unidade de investigação, o acolhimento oferecido e as facilidades concedidas para a realização do trabalho que tenho usado desde o início do meu mestrado em 2001. Agradeço também aos colegas do Instituto de Telecomunicações pelos comentários relevantes e pela disponibilidade para discutir aspectos do trabalho.

Agradeço à Escola Superior de Tecnologia e Gestão de Águeda pela possibilidade de efectuar concentração de serviço docente durante dois anos lectivos, permitindo dedicação exclusiva aos trabalhos do doutoramento durante dois semestres, bem como pela isenção de propinas de doutoramento.

Por último agradeço à Fundação para a Ciência e Tecnologia pelo apoio que me deu nas despesas de participação na "*16th International Conference on Telecommunications*".

A todos, muito obrigado.

palavras-chave

Gestão de redes, Qualidade de Serviço, Redes de Próxima Geração.

resumo

A evolução observada nas redes de comunicações durante a última década traduziu-se na diversificação de serviços que utilizam a rede, no aumento das taxas de transferência e na massificação da utilização de serviços de acesso à Internet e de comunicações celulares.
Durante esta década, várias organizações, das quais se destacam os operadores de telecomunicações, têm dedicado consideráveis esforços no sentido de definir e normalizar arquitecturas de redes de próxima geração. A principal característica deste tipo de rede reside no facto de possuir uma arquitectura modular capaz de fornecer serviços multimédia a clientes de uma rede de acesso com características tecnológicas heterogéneas. Os trabalhos de normalização das arquitecturas de rede NGN têm-se limitado, até ao momento, a especificar detalhes relativos ao funcionamento da rede não tendo ainda sido definida a arquitectura de gestão.
Em termos de tecnologias de gestão de redes, foram propostos nas últimas duas décadas novos paradigmas de gestão, novos modelos de dados, novos protocolos de transporte e várias linguagens de definição de informação de gestão. Os modelos de dados têm vindo a ser enriquecidos, os protocolos são mais flexíveis e poderosos, as soluções de gestão oferecem interoperabilidade acrescida e as linguagens permitem definir formatos de configuração mais ricos. Simultaneamente tem crescido a complexidade das soluções de gestão, aumentado a sobrecarga causada pelo aumento de complexidade nos equipamentos bem como nas plataformas computacionais que suportam os sistemas de gestão.
O presente trabalho propõe uma solução de gestão para redes NGN capaz de gerir os recursos de rede garantindo Qualidade de Serviço. A solução de gestão proposta inclui uma plataforma de execução de políticas que utiliza os eventos ocorridos na rede para empreender acções de configuração, autonomizando o processo de gestão. Inclui uma avaliação da complexidade de várias tecnologias de gestão estudando a sobrecarga causada pela tecnologia tanto no processo de gestão como na operação da rede. É ainda estudada a escalabilidade das várias tecnologias e analisado o seu comportamento num cenário da rede de um operador de telecomunicações. O trabalho propõe ainda uma metodologia de configuração integrada dos elementos de gestão, através de uma interface de configuração amigável para o administrador do sistema.

keywords Network Management, Quality of Service, Next Generation Networks

abstract

The evolution occurred in the communication networks during the last decade can be observed in the network service diversity, in the increase of the network transmission rates and in the wide usage of the internet access and cellular communication services.
During the last decade several standardization bodies, that have a strong participation of the telecommunication operators, dedicated considerable efforts to develop an architecture for the next generation networks. The main attribute of this kind of networks is that it consists in a modular architecture able to provide multimedia services to the clients of a heterogeneous access network. The NGN architecture standardization efforts have been so far focused on the operational details of the network, leaving the network management details to be defined in the near future.
In terms of network management technologies, the last two decades brought new management paradigms, new data models, new transport protocols and new languages to specify the management information.
The data models have been improved, new the management protocols are more flexible and powerful, the newer management solutions offer an extra interoperability and the management languages allow to define richer configuration models. Simultaneously the complexity of the management solutions has been increased, as well as the overhead cause by the management technologies in the network equipments and in computational systems that implement the management systems.
Current work proposes a management solution for the NGN networks, capable to manage their network resources, allowing Quality of Service guaranties. The proposed solution includes a policy execution platform that uses the events occurred inside the network in order to trigger configuration actions, automating the management process. Present work includes a complexity evaluation of several management technologies, studying the overhead each technology causes both in the management process and in the network operation. The scalability of the technologies is studied as well and it analyzed its behavior in an operator network scenario. It is proposed an integrated configuration methodology of the management elements, by means of a user friendly configuration interface.

Índice de Figuras

Índice de Tabelas

Lista de acrónimos

ACRÓNIMO	SIGNIFICADO
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AAAC	Authentication, Authorization, Accounting and Charging
AF	Assured Forwarding Service
ANACOM	Autoridade Nacional de Telecomunicações
AR	Router de acesso
AS	Autonomous System
ASAP	As Soon As Possible
ASN.1	Abstract Syntax One
AUP	Atribute Value Pair
BA	Behaviour Aggregate
BB	Bandwidth Broker
BE	Best Effort
BEEP	Blocks Extensible Exchange Protocol
BGP	Border Gateway Protocol
BNF	Backus Naur Form
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CIMOM	CIM Object Manager
CLI	Command Line Interface
CMIP	Common management information protocol
CMS	Cryptographic Message Syntax
COPS	Common Open Policy Service
CQL	CIM Query Language
DAP	Directory Access Protocol
DAS	Directory Server Agent
DEN	Directory Enabled Networks
DEN-ng	Directory Enabled Networks Next Generation
DiffServ	Differentiated Services
DMI	Desktop Management Information
DMTF	Distrbutted Management Task Force
DNF	Disjuntive Normal Form
DSCP	DiffServ Service Code
DVB/DAB	Acesso via broadcast
ECA	Event-Condition-Action
EF	Expedited Forwarding Service
FCAPS	Fault Configuration Accounting Performance Security
FEC	Forwarding Equivalence Class
FP5	Framework Programm 5
FP6	Framework Programm 6
GSM	Groupe Special Mobile
HTTP	HyperText Transfer Protocol
I&D	Investigação e Desenvolvimento
IAB	Internet Architecture Board
IETF	Internet Engineering Task Force
IMS-IP	Multimédia subSystem
IntServ	Integrated Services
IP	Internet Protocol
IPSec	Internet Protocol Security
IPV6	Internet Protocol Version 6
IST	Internet Society Tecnologies
ITU-T	Telecommunication Standardization Sector da International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol

LER	Laber Edge Router
LPDP	Local Policy Definition Point
LS	Label Switching
LSP	Label Switching Path
LSR	Label Switching Router
MIB	Management Information Base
MIPL	Mobile IP Linux
Mobile VCE	Virtual Center of Excellence in Mobile and Personal Communications
Moby Dick	Mobility and Differentiated Services in a Future IP Network
MOF	Managed Object Format
MPLS	Multiprotocol Label Switching
MUWS	Management Using Web Services
NASREQ	Network Access Server REQuirements
NGOSS	New Generation Operations Systems and Software
OID	Object IDentification
PAN	Personal Area network
PBM	Policy Based Management
PBNM	Polivy Based Network Management
PCIM	Policy Common Information Model
PCIMe	Policy Common Information Model Extensions
PDP	Policy Definition Point
PEP	Policy Enforcement Point
PHB	Per Hop Behaviour
PIB	Policy Information Base
PPP	Ligações Ponto-a-Ponto
PRC	PRovioning Classes
PRI	PRovioning Instances
PRID	PRovisioning Indentifier
QDDIM	QoS Device Datapath Information Model
QdS	Qualidade de Serviço
QPIM	Policy Quality of Service (QoS) Information Model
RADIUS	Remote Authentication Dial In User Service
RAP	Resource Allocation Protocol
RELAX NG	REgular LAnguage for XML Next Generation
RESV	Reservation message
RFC	Request For Comments
RMON	Remote Network MONitoring
RND	Relative Distinguished Name
RPC	Remote Procedure Calls
RSVP	Resource ReSerVation Protocol
SIP	Session Initiation Protocol
SMIng	Struture Management Information next Generation
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SPL	Simplified Policy Language
SSH	Secure Shell
TCP	Transmission Control Protocol
TD-CDMA	Time Division Code Division Multiple Access
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
TOS	Type Of Service
TSPEC	Traffic Specification
TTL	Time To Live
UDP	User Datagram Protocol
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
VOIP	Voice Over IP
WBEM	Web-Based Enterprise Management
WCDMA	Wide-Band Code-Division Multiple Access
WiFI	Wireless FIdelity

WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WWRF	World Wireless Research Forum
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

1 Introdução

A dimensão da rede de um operador de comunicações e a heterogeneidade dos equipamentos que a compõem transformam a sua gestão numa tarefa complexa, onerosa, repetitiva, e sujeita a erros. As acções de configuração têm que ser levadas a cabo em todos os equipamentos de rede, dispersos, muitas vezes, por uma extensa área geográfica. A configuração dos equipamentos requer a utilização de mão-de-obra muito especializada, com vasto conhecimento da rede e respectivo funcionamento e um profundo conhecimento do equipamento, bem como da sua configuração. Adicionalmente, devido a questões comerciais, os fabricantes de equipamentos de rede disponibilizam mecanismos proprietários de configuração dos seus equipamentos, que muitas vezes diferem até entre modelos. A especificidade dos suportes de configuração dos equipamentos e a complexidade das acções de configuração, tornam as tarefas de gestão de redes muito complexas e muito sujeitas a erro quando efectuadas por um operador humano.

Os erros de configuração traduzem-se tipicamente em indisponibilidade ou em mau funcionamento dos serviços que, por sua vez, origina prejuízos e descontentamento entre os utilizadores da rede.

Graças ao dinamismo actual do mercado das comunicações, as alterações das características dos serviços fornecidos pelos operadores, implicam configurações frequentes dos diversos equipamentos. Essas acções de configuração necessitam de ser efectuadas à escala da rede do operador e nas várias vertentes de cada serviço como, por exemplo, no suporte de registo de utilização ou nos elementos de transporte.

A complexidade deste cenário de gestão requer a utilização de mecanismos automáticos que efectuem a configuração autónoma e coordenada de todos os equipamentos da rede, minimizando o factor de erro associado à intervenção humana.

1.1 Enquadramento

A gestão de rede baseada em políticas é um paradigma de gestão, que consiste na definição de regras para determinar o comportamento de um sistema. As soluções de gestão baseadas em políticas contemplam, entre outras coisas, um servidor de gestão que se encarrega de efectuar a configuração dos equipamentos do seu domínio de gestão, garantindo acções de configuração integrada, sem erros e com custos reduzidos.

As redes da próxima geração (*Next Generation Network* - NGN) têm sido um tópico de intensa investigação e a sua arquitectura tem vindo a ser definida por organizações como a ITU-T (*Telecommunication Standardization Sector* da *International Telecommunication Union)*, o 3GPP (*Third Generation Partnership Project)*, e o TISPAN (*Telecommunications and Internet converged Services and Protocols for Advanced Networking)*. O conceito de rede NGN resume-se a uma plataforma modular capaz de fornecer serviços multimédia a clientes de redes móveis, integrando serviços de voz com serviços de dados, bem como tecnologias de rede móvel com as da rede fixa.

O 3GPP tem vindo desde 1999 a propor sucessivas versões da arquitectura de rede NGN, definindo entidades funcionais e as suas interfaces de comunicação. Existem já vários produtos comerciais desenvolvidos segundo as suas especificações.

Apesar de existirem várias arquitecturas de rede NGN, uma por cada entidade normalizadora, todas elas são constituídas por uma plataforma modular que separa a gestão dos serviços da gestão da rede de transporte. Todas elas convergem também na utilização de um componente designado de *IP Multimedia Subsystem* que foi desenvolvida pelo 3GPP.

No que respeita à componente de gestão de rede NGN, os trabalhos estão mais atrasados do que em relação à componente funcional da rede; foram somente definidos requisitos de gestão e proposta uma arquitectura de gestão muito vaga e baseada no modelo de gestão *Telecommunications Management Network* (TMN).

Têm vindo a ser desenvolvidas nas últimas duas décadas várias tecnologias de gestão de redes, mais poderosas, mais flexíveis, com maior interoperabilidade e, consequentemente, com maior complexidade e maior sobrecarga computacional. A sobrecarga manifesta-se, quer nos elementos pertencentes à plataforma de gestão, quer nos elementos geridos, reflectindo-se nos requisitos de processamento, de memória, bem como na quantidade de tráfego de gestão produzido.

Num cenário de gestão de grandes dimensões, como é exemplo uma rede NGN, onde os elementos de rede oferecem geralmente reduzidas capacidades computacionais, é necessário avaliar cuidadosamente o equilíbrio entre as capacidades oferecidas pelas tecnologias de gestão e a sobrecarga por elas provocada; sob pena de comprometer o desempenho da própria rede e reduzir a sua escalabilidade.

1.2 Objectivos

O grande objectivo deste trabalho é estudar e aplicar tecnologias de gestão de redes numa plataforma de gestão de um operador de rede NGN, especialmente no que se relaciona com a gestão de Qualidade de Serviço.

Pretende-se avaliar as diversas tecnologias de gestão, verificando a complexidade e a sobrecarga relacionada com a sua utilização. Pretende-se ainda verificar a adaptabilidade que cada uma das tecnologias apresenta para os diversos elementos do cenário de gestão.

Adicionalmente pretende-se propor uma arquitectura de gestão modular e implementar uma solução de gestão de redes NGN que, utilizando o paradigma de gestão baseada em políticas, seja capaz de efectuar a gestão dos recursos de rede, fornecendo garantias de qualidade de serviço. A solução de gestão a propor deve ser escalável e deverá ser aplicável a um cenário de gestão de grande dimensão. Deve implementar um modelo de refinamento das políticas de forma a adequar o formato das políticas de rede a cada uma das camadas de gestão do sistema proposto.

É ainda objectivo desta tese definir uma plataforma de execução de políticas dinâmica que permita despoletar automaticamente a execução de acções de reconfiguração em resposta a eventos ocorridos na rede.

Pretende-se, finalmente, propor uma metodologia de configuração integrada dos elementos de gestão fazendo uso de uma interface de configuração amigável, de forma a facilitar a interacção do administrador do sistema com toda a plataforma de gestão.

1.3 Contribuições relevantes

O principal contributo do trabalho de doutoramento que está na base da presente dissertação é a definição de uma nova arquitectura de gestão para redes NGN.

Assim constituem contribuições relevantes do presente trabalho:

- uma arquitectura original, escalável e modular de gestão baseada em políticas para a gestão de redes NGN;
- uma avaliação da complexidade e sobrecarga causadas pelas tecnologias de gestão mais utilizadas, tanto em processos de gestão, como em processos de operação da rede;
- um estudo de escalabilidade das diversas tecnologias e análise do seu comportamento num cenário de rede de um operador de telecomunicações;
- uma plataforma de execução de políticas que tem em conta os eventos da rede para empreender acções de configuração, autonomizando o processo de gestão;
- uma metodologia de configuração integrada dos elementos de gestão através de uma interface de configuração amigável para o administrador do sistema.

Foram publicadas no âmbito do presente trabalho as seguintes publicações:

1. P. Gonçalves, C. Figueira, R. Azevedo, R. Aguiar, and J. L. Oliveira, "*A graphical user interface for policy composition in CIM-SPL*" in IEEE International Workshop on

Management of Emerging Networks and Services - MENS 2009, St.-Petersburg, Russia, 2009.

2. P. Gonçalves, R. Azevedo, J. L. Oliveira, and R. Aguiar, "*Managing QoS in a NGN using a PBM approach*" in The Fourth International Conference on Systems and Networks Communications- ICSNC 2009 Porto, Portugal, 2009.
3. P. Gonçalves, R. Azevedo, D. Gomes, J. L. Oliveira, and R. L. Aguiar, "*Evaluation of Policy Based Admission Control Mechanisms in NGN*", in International Conference on Telecommunications 2009, Marrakech, Morocco, 2009.
4. P. Gonçalves, J. L. Oliveira, and R. L. Aguiar, "*An evaluation of network management protocols*", in 11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), New York, USA, 2009.
5. S. Sargento, R. Prior, F. Sousa, P. Gonçalves, J. Gozdecki, D. Gomes, E. Guainella, A. Cuevas, W. Dziunikowski, and F. Fontes, "*End-to-end QoS Architecture for 4G Scenarios*", in 14th IST Mobile & Wireless Communications Summit (IST Summit 2005), Dresden, Germany, 2005.
6. J. L. Oliveira, P. Gonçalves, W. Dziunikowski, J. Wszolek, S. Rasmussen, R. P. Lopes, and V. Roque, "*Policy-Based Network Management in an Integrated Mobile Network*", in Advanced Industrial Conference on Telecommunications, Lisbon, Portugal, 2005.
7. P. Goncalves, J. L. Oliveira, and R. L. Aguiar, "*A WBEM based solution for a 4G network integrated management*", in Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, 2005.
8. W. Dziunikowski, J. Wszolek, P. Gonçalves, S. Rasmussen, A. Cuevas, R. P. Lopes, V. Roque, and J. L. Oliveira, "*Using CIM Extensions to model Managed Entities in Heterogeneous Networks*", in IEEE International Workshop on Management Issues and Challenges in Mobile Computing, Nice, France, 2005.

1.4 Organização do documento

Para além deste primeiro capítulo introdutório a dissertação está estruturada em mais cinco (Figura 1.1).

O segundo capítulo faz o levantamento do estado da arte no que respeita à tecnologia de gestão de redes: descreve o paradigma da gestão baseado em políticas, faz o levantamento dos principais protocolos de comunicação utilizados para implementar a comunicação dos elementos de

gestão, dos modelos de dados que representam a informação de gestão, e das mais importantes linguagens de definição de políticas propostas.

O capítulo 3 faz um levantamento do estado da arte na área das arquitecturas de redes de próxima geração, descrevendo as mais representativas: descreve a evolução do conceito associado às redes de próxima geração; descreve as arquitecturas de rede de próxima geração; e descreve as tecnologias mais relevantes que são utilizadas na gestão das redes e dos serviços.

O capítulo 4 descreve a arquitectura da solução de gestão proposta: são analisados os requisitos de gestão de uma rede NGN; são identificados e descritos os elementos da arquitectura proposta; são identificadas as tecnologias e protocolos de comunicação utilizados; é descrita a interacção entre as entidades do cenário de gestão; e é descrito o processo de configuração do sistema.

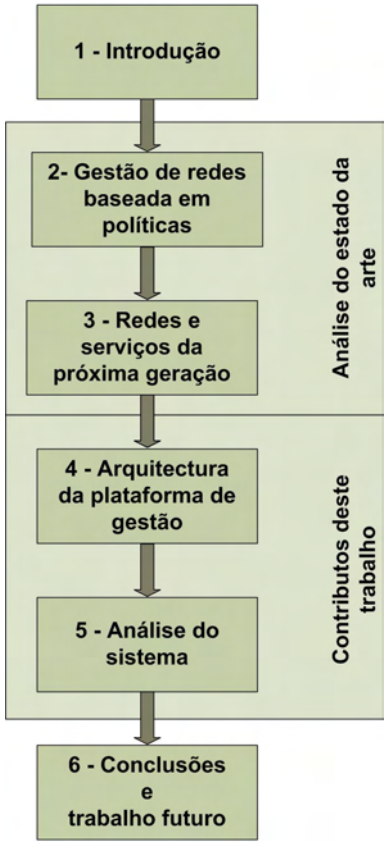

Figura 1.1- Estrutura da dissertação.

O capítulo 5 descreve a análise efectuada ao sistema desenvolvido: é analisado o comportamento do sistema central de gestão para diferentes volumes de carga, de forma a comprovar a sua escalabilidade e consequente possibilidade de utilização num cenário de gestão com a dimensão de um operador de comunicações; é analisado o desempenho das interfaces de interligação dos elementos pertencentes às três camadas da arquitectura proposta; são comparadas

tecnologias de gestão alternativas e é estudada a sua adequabilidade ao cenário de gestão; e é analisada a escalabilidade dos vários componentes do sistema de gestão.

Finalmente o capítulo 6 apresenta as principais conclusões que saíram deste trabalho e identifica ainda algumas possibilidades de investigação para o futuro.

2 Gestão de redes baseada em políticas

A complexidade crescente dos equipamentos de redes obriga à optimização das operações de gestão e de configuração dos equipamentos. No processo de criação de um novo serviço um operador de telecomunicações necessita de configurar simultaneamente os equipamentos de gestão de utilizadores, os *proxies* da rede, os servidores de conteúdos e todos os *routers* pertencentes ao domínio. A configuração inconsistente dos equipamentos pode levar a falhas nos sistemas e consequentemente a falhas na prestação dos serviços. Apesar das consequências que podem ter, essas inconsistências são extremamente difíceis de detectar, especialmente se a rede for de grandes dimensões. Outro factor de risco é a imensa quantidade de equipamentos a configurar obrigando a um trabalho muito repetitivo e pouco adequado a um operador humano, pela tendência deste para errar na execução de tarefas repetitivas.

Foram várias as organizações que se envolveram na investigação e na normalização de arquitecturas, de modelos de dados e de linguagens de especificação de políticas, nomeadamente as que estão associadas ao *Internet Engineering Task Force* (IETF) e *Distributed Management Task Force* (DMTF). Na Figura 2.1 sintetizámos algumas das tecnologias desenvolvidas durante os últimos 20 anos e que serão discutidas ao longo deste capítulo. A organização contempla as entidades de normalização os modelos de dados, as metodologias de codificação da informação de gestão e os protocolos de transporte.

Neste capítulo descreve-se o paradigma de gestão baseada em políticas, analisam-se os principais modelos de gestão de redes e sistemas, descrevem-se as metodologias de codificação da informação de gestão, analisam-se os protocolos de transporte de informação de gestão e examinam-se ainda algumas linguagens de definição de políticas, especialmente as que apresentam maior potencial para a área de gestão de redes.

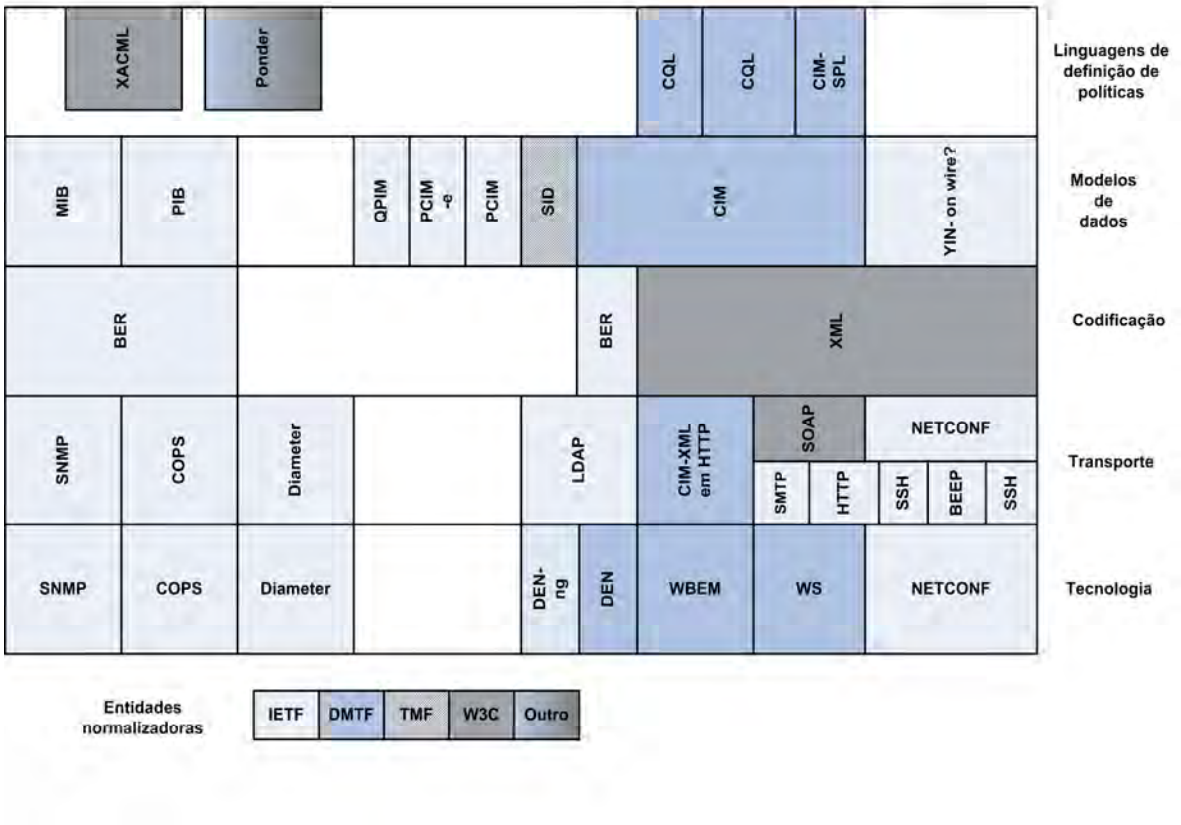

Figura 2.1 - Tecnologias de gestão de redes e sistemas.

2.1 Paradigma de gestão baseada em políticas

A gestão baseada em políticas (*Policy Based Management* - PBM) [1] consiste na definição de regras que estabelecem o comportamento de um sistema. O paradigma de gestão PBM propõe que a configuração dos equipamentos seja efectuada com base num conjunto de regras (políticas) que governam o comportamento de todo o equipamento gerido. O operador humano faz a definição das políticas junto do servidor de gestão e este encarrega-se de efectuar de uma forma automática a configuração de todos os equipamentos pertencentes ao sistema.

Apesar de na literatura aparecer apresentada em vários formatos e para uma grande diversidade de aplicações [2], podemos ver uma política, como uma regra constituída por componentes pré-definidos. Na sua forma mais vulgar a política inclui uma condição que é avaliada e um conjunto de acções que são executadas quando a regra é aplicada:

```
Politica ::= if <condição> then <acção>                    (1)
```

Existem, no entanto, outros formatos de especificação de políticas onde se adiciona à regra um terceiro componente na forma de um evento que despoleta a avaliação da condição, segundo um modelo designado de ECA (*Evento, Condição e Acção*) [3].

Como exemplo de uma política pode-se considerar a regra seguinte que especifica que quando o protocolo de transporte for UDP se deve reservar 30% da largura de banda disponível:

```
if <IP protocol is UDP> then < guarantee 30% of available BW >        (2)
```

As condições podem ser agrupadas através de conjunções ou disjunções de condições simples constituindo assim novas condições mais complexas. Da mesma forma, as acções constantes nas políticas podem ser agrupadas definindo conjuntos de acções a ser executadas.

As políticas são independentes dos dispositivos e da sua implementação, definindo apenas o seu comportamento em termos abstractos. São implementadas centralmente pela plataforma de gestão que se encarrega de as aplicar a todos os elementos a gerir, podendo ser traduzidas entre os elementos de diferentes camadas de um sistema PBM segundo um processo designado por *policy continuum* [3] ou ainda por adaptação de políticas [4].

Algumas das vantagens normalmente atribuídas ao paradigma PBM são: a configuração facilitada dos equipamentos, a eliminação do factor de erro introduzido pela intervenção humana nas acções de configuração; a diminuição do tempo de resposta às operações de alteração na configuração dos equipamentos; a configuração integrada das entidades a gerir à escala do domínio de gestão, independentemente da dimensão ou heterogeneidade das mesmas; a possibilidade de implementação de transacções nas acções de configuração, bem como a possibilidade de integração das acções de gestão com as regras de gestão das organizações.

2.2 Linguagens de definição de políticas

Nos últimos anos várias linguagens de especificação de políticas têm sido propostas [2]. Nesta secção são descritas duas soluções: Ponder [5] e *CIM Simplified Policy Language* (CIM-SPL) [6].

2.2.1 Ponder

Ponder é uma linguagem de especificação de políticas proposta por uma equipa do *Imperial College* de Londres [7]. A linguagem é declarativa, orientada a objectos, e permite a definição de políticas para um amplo conjunto de áreas da gestão, desde o controlo de admissão até à configuração de equipamentos. Nesta proposta as políticas são divididas em dois grupos [7]: o primeiro constituído pelas políticas de controlo de acesso, subdividido num conjunto de outros subtipos como autorização (*authorisation policies)*, delegação (*delegation policies)*, filtragem de

informação (*information filtering)* e repressão (*refrain policies)*; e o segundo constituído pelas políticas de obrigação (*obligation policies*). A linguagem utiliza sistematicamente três conceitos: o *subject* que representa um sujeito ou um utilizador, humano ou um componente autónomo, que possui responsabilidade em termos de gestão; o *target* que representa recursos ou fornecedores de recursos sobre os quais recaem as regras das políticas; e os *domains* representam uma forma de agregação de objectos utilizada pela linguagem.

As políticas de autorização definem as actividades que um elemento do tipo *subject* está autorizado a executar sobre os objectos do tipo *target*. São políticas de controlo de acesso que visam proteger os recursos e serviços do acesso não autorizado, por parte dos utilizadores. Existem políticas de autorização positiva que permitem o acesso a objectos, bem como políticas de autorização negativa que negam o acesso a objectos.

A Figura 2.4 ilustra a sintaxe das políticas de autorização em Ponder, onde as palavras em negrito representam termos reservados da linguagem. Na linguagem, os componentes de uma política não necessitam seguir uma determinada ordem.

```
inst ( auth+ | auth- ) policyName "{"
subject [<type>] domain-Scope-Expression ;
target [<type>] domain-Scope-Expression ;
action action-list ;
[ when constraint-Expression ; ] "}"
```

Figura 2.2 - Sintaxe de uma política de autorização.

As políticas de filtragem de informação, cuja sintaxe se ilustra na Figura 2.3, servem para transformar informação de entrada ou de saída em parâmetros de uma acção. Implementam um conceito semelhante ao das vistas das bases de dados onde, através de consultas, se criam relações virtuais temporárias que filtram a informação de uma outra relação ou ainda de um conjunto de relações. A utilização de políticas de filtragem está limitada a políticas de autorização positiva.

Cada acção pode ser associada com um número de expressões de filtragem e cada filtro pode conter uma condição para a sua própria aplicação. Quando a expressão é avaliada como verdadeira, as acções de atribuição constantes do corpo do filtro serão executadas. As palavras reservadas *in* e *out* indicam se são de entrada ou de saída os parâmetros que são passados ao corpo do filtro. A palavra reservada *result* é usada para armazenar o valor de retorno da acção executada.

```
actionName { filter }
filter = [ if condition ] "{" { ( in parameterName = expression ; |
                          out parameterName = expression ; |
                                  result = expression ; ) } "}"
```

Figura 2.3 - Sintaxe de uma política de filtragem de informação.

As políticas de delegação servem para temporariamente transmitir autorizações de direitos de acesso e estão intimamente associadas às políticas de autorização especificando os direitos de acesso que são delegados noutros sujeitos. Este tipo de política permite transferir os direitos que

um sujeito possui para que outro sujeito possa executar uma acção em representação do primeiro. As políticas de delegação negativas proíbem a delegação de privilégios. Permitem definir um conjunto de condições através das suas componentes: constrangimentos temporais para a delegação através da componente *when*; e constrangimentos condicionais através da utilização de uma condição na componente *valid*. Só as políticas de delegação positiva podem incluir estes constrangimentos no processo de delegação. A delegação de privilégios está limitada ao conjunto de privilégios possuídos pelo primeiro sujeito, só podendo ser delegados e revogados direitos possuídos.

```
inst deleg+ "("associated-auth-policy ")" policyName "{"
grantee [<type>] domain-Scope-Expression ;
[ subject [<type>] domain-Scope-Expression ; ]
[ target [<type>] domain-Scope-Expression ; ]
[ action action-list ; ]
[ when constraint-Expression ; ]
[ valid constraint-Expression ; ] "}"
```

Figura 2.4 - Sintaxe de uma política de delegação.

As políticas de repressão, cuja sintaxe se ilustra na Figura 2.4, definem acções que os sujeitos devem abster-se de executar sobre os objectos alvo, mesmo que tenham permissões para as executar. Actuam como repressores sobre as acções que os sujeitos executam sobre os alvos. Consistem num conceito muito semelhante ao conceito implementado pelas políticas de autorização negativa, com a única diferença de que são aplicadas sobre os sujeitos em vez de serem aplicadas pelos controladores de acesso, como no caso das políticas de autorização negativa.

As políticas de obrigação representam acções que devem ser executadas pelos gestores de um sistema, quando determinados eventos ocorrem para que este possa responder à mudança de circunstâncias. São desencadeadas por eventos e definem actividades que os sujeitos devem executar sobre os objectos de um domínio.

Na sintaxe das políticas de obrigação, ilustrada na Figura 2.5, a palavra reservada *on* precede à definição do evento que despoleta a verificação da política. A componente *target* é opcional, uma vez que as acções podem ser executadas sobre o sujeito definido na política; caso contrário deve ser definido na expressão da política. A lista de acções a serem executadas pela política é definida na componente *do*. As políticas de obrigação permitem ainda definir a excepção que deve ser criada se acções definidas na política falharem, bem como a definição de alguns constrangimentos à execução da política (componente *when)*.

Uma das componentes mais importantes de uma política é o conjunto de condições segundo as quais a política deva ser executada. Essas condições podem, no entanto, depender da existência ou execução simultânea de outras políticas. Por isso o Ponder divide os constrangimentos à execução das políticas em constrangimentos destinados a políticas simples e em constrangimentos destinados a grupos de políticas, a que chama meta-políticas.

```
inst oblig policyName "{"
on event-specification ;
subject [<type>] domain-Scope-Expression ;
[ target [<type>] domain-Scope-Expression ; ]
do obligation-action-list ;
[ catch exception-specification ; ]
[ when constraint-Expression ; ] "}"
```

Figura 2.5 - Sintaxe de uma política de obrigação.

Os constrangimentos para políticas simples limitam a aplicação de uma política simples. São expressos com base num predicado que deve ser avaliado como verdadeiro para que a política seja executada. Os constrangimentos para grupos de políticas são conjunções de constrangimentos simples que podem incluir: informação acerca do estado do sujeito ou alvo da política; parâmetros acerca das acções e eventos; ou ainda constrangimentos temporais que especifiquem períodos de validade da política.

As meta-políticas especificam políticas acerca de políticas dentro de uma política composta, definindo constrangimentos relativos à execução das políticas. São tipicamente especificadas para grupos de políticas de forma a definir constrangimentos que limitam as políticas permitidas num sistema, ou para desabilitar a execução simultânea de políticas incompatíveis.

A linguagem Ponder suporta dois mecanismos de agregação: a criação de grupos de políticas e a criação de papéis (*roles*). Em Ponder um grupo pode conter zero ou mais políticas, e outros grupos de políticas num esquema de encapsulamento de políticas bem como meta políticas, com uma sintaxe como a ilustrada na Figura 2.6. A linguagem permite ainda que os grupos sejam constituídos como tipos podendo assim ser instanciados sempre que necessário.

```
inst group groupName "{"
   { basic-policy-definition }
   { group-definition }
   { meta-policy-definition } "}"
```

Figura 2.6 - Sintaxe de definição de grupos em Ponder.

Os papéis fornecem um mecanismo de agrupamento de políticas que possuam um mesmo sujeito, tipicamente associado a uma função desempenhada dentro de uma organização (*e.g.:* gestor de projecto, analista, …). Tal como acontece em relação aos sujeitos das políticas simples, os papéis podem ser atribuídos a outros sujeitos actores de gestão não humanos, como gestores de recursos ou outros.

A sintaxe de criação de papéis, ilustrada na Figura 2.7, permite a inclusão de um qualquer número de políticas básicas, de grupos ou mesmo de meta políticas. Permite a representação dos cargos de uma organização como domínios de sujeitos que podem ser utilizados na especificação do papel logo a seguir ao caracter '@'.

```
inst role roleName "{"
   { basic-policy-definition }
   { group-definition }
   { meta-policy-definition } "}" [ @ subject-domain ]
```

Figura 2.7 - Sintaxe de definição de papéis em Ponder.

Devido às características de linguagem orientada a objectos, Ponder permite ainda implementar heranças de tipos, de acordo com uma hierarquia ilustrada na Figura 2.8.

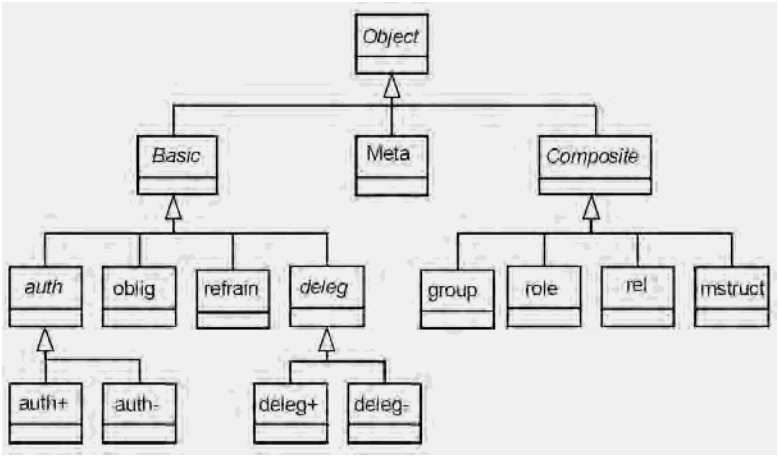

Figura 2.8 - Hierarquia de objectos Ponder.

2.2.2 CIM Simplified Policy Language (CIM-SPL)

CIM Simplified Policy Language (CIM-SPL) [8] é uma linguagem de especificação de políticas proposta por Agrawal *et al* [6] no seio do DMTF. Trata-se de uma linguagem declarativa que utiliza o CIM Policy Model como modelo de representação de dados, permitindo a especificação de políticas no formato *if-condition-then-action*. Permite a escrita de políticas, cujas condições incluam dados CIM que descrevam as propriedades dos recursos geridos. A componente de acção de uma política SPL pode invocar operações ou métodos, por exemplo de objectos CIM presentes no servidor de gestão CIM. O elemento principal de uma política SPL é a regra, cuja estrutura se encontra ilustrada na Figura 2.9.

A instrução *import* inclui uma classe CIM designada de classe âncora, cujos métodos e propriedades se encontram disponíveis na regra. A regra pode também aceder a outros objectos CIM, mas só no caso de a classe âncora participar através de uma relação ou conjunto de relações de associação. A linguagem SPL implementa o mesmo tipo de agregação disponível em CIM. Utiliza conceitos como grupos de políticas, permitindo uma organização hierárquica das políticas de acordo com as suas funcionalidades, a sua importância, o seu âmbito de aplicabilidade, ou até imitando a organização hierárquica das entidades geridas.

```
Import <MOF Name>::<CIM Class Name>:<Condition>
Strategy <execution strategy>
Declaration {
        <constant definition>
        <macro definition>
}
Policy{
Declaration { <constants and macros> }
Condition {<boolean expression>}
Decision {<action workflow>}
}:<Priority>;
```

Figura 2.9 – Estrutura de uma regra SPL.

A secção *declaration* é uma secção opcional onde se definem macros e constantes permitindo a reutilização dos elementos definidos, simplificando a edição das expressões das condições e acções. Permite ainda encurtar a extensão das expressões nas condições devido ao tamanho considerável dos nomes dos objectos do modelo CIM.

Em CIM-SPL uma política diz-se aplicável se a sua condição for considerada verdadeira, enquanto que um grupo de políticas diz-se aplicável se pelo menos uma das suas políticas for aplicável. A instrução de *strategy* é aplicável a cada grupo de políticas definindo a estratégia de execução das acções da política. Apesar de poderem existir outras estratégias de execução, são obrigatórias as implementações das estratégias *Execute_All_Applicable* e *Execute_First_Applicable*. A primeira obriga à avaliação de todas as políticas aplicáveis, enquanto que a segunda testa a avaliação das políticas segundo a ordem de prioridade, até encontrar uma que seja aplicável.

Cada política contém uma secção opcional de declaração que segue as mesmas regras que a secção de declarações global, mas com uma diferença: uma declaração feita dentro da área de declarações de uma política tem um âmbito limitado à política mas com prioridade em relação a uma declaração feita globalmente.

Na secção *condition* são especificadas as condições a verificar para que a política seja executada. Contém uma expressão booleana composta por operadores aritméticos em conjunto com operadores como AND, OR ou NOT, bem como propriedades dos objectos CIM acessíveis da classe âncora. A linguagem SPL permite a composição de condições constituídas por conjunções e disjunções de sub-condições, desde que a expressão resultado continue a constituir uma condição booleana.

As acções presentes nas políticas SPL são incluídas na secção *decision*, sendo na sua maioria a invocação dos métodos dos objectos acessíveis da classe âncora, mas também a edição dos valores das propriedades da classe âncora. O CIM-SPL permite também a composição de acções simples em acções mais complexas, podendo ser executadas em série ou de forma concorrente. Permite ainda a execução de novas políticas como acção de uma outra política, no

processo designado de políticas em cascata. A Figura 2.10 ilustra um exemplo de uma regra completa.

```
Import Class org.apache.imperius.javaspl.samples.simplepolicies.UA_Policy:pol;
Strategy Execute_All_Applicable;
Policy
{
        Declaration
        {
                dstAddr = "2001:690:2380:777a:20c:29ff:fe7e:4727";
        }
        Condition
        {
                (pol.addCond(IPCLASSIFIER, DSTADDR, dstAddr) == true)
        }
        Decision
        {
                pol.setName("Block destination")
                pol.setPrio(3)
                pol.setCondStyle(1)
                pol.addAction("Drop")
        }
}:3;
```

Figura 2.10 - Exemplo de política em CIM-SPL.

A linguagem CIM-SPL suporta a definição de grupos de políticas de modo a permitir uma organização do código mais eficiente (Figura 2.11). Os grupos podem conter outros grupos e têm de conter pelo menos uma política ou um grupo. Tal como acontece em relação à definição das políticas, a linguagem obriga a que os grupos incluam a definição da sua prioridade, na forma de um valor inteiro positivo, que deve ser única entre todos os grupos de políticas. Os grupos podem conter também instruções de *Import,* definido classes âncora próprias, bem como secções autónomas destinadas a efectuar a declaração de macros e constantes.

```
Import CIM_V<major>_<minor>_<release><final or preliminary><mof file name w/o
extension>::<class name>:<simple Boolean condition> ;
Strategy [Execute_All_Applicable | Execute_First_Applicable] ; (Obrigatório)
Declaration {
<List of constant definition> (Opcional)
<List of macro definitions> (Opcional)
}
Policy { … } : Priority; (Opcional)
Policy { … } : Priority; (Opcional)
Policy { … } : Priority; (Prioridade Obrigatória)
…
PolicyGroup:[Association Name(Property1,Property2)] { … }: Priority;
 (Opcional)
PolicyGroup:[Association Name(Property1,Property2)] { … }: Priority;
 (Opcional)
PolicyGroup:[Association Name(Property1,Property2)] { … }: Priority;
 (Opcional)
```

Figura 2.11 - Sintaxe de definição de grupos em CIM-SPL.

2.3 Tecnologias de gestão de redes

A definição de políticas pode ser realizada a um nível abstracto relativamente à tecnologia de gestão que garante a operacionalidade. No entanto, o seu impacto depende naturalmente dos protocolos de transporte e dos modelos de dados utilizados.

Nesta secção descrevem-se algumas tecnologias de gestão de redes desenvolvidas pelo IETF e DMTF desde a introdução do protocolo SNMP no fim dos anos 80.

2.3.1 Simple Network Management Protocol (SNMP)

Durante a década de 80 o IETF desenvolveu um novo modelo de gestão baseado no protocolo *Simple Network Management Protocol* (SNMP) [9], com o objectivo de disponibilizar uma forma simples e prática de realizar a gestão e a monitorização de elementos de rede. A filosofia que esteve na base da concepção de toda a arquitectura de gestão foi a simplicidade: as capacidades computacionais dos elementos de rede eram limitadas (e ainda hoje são) e importava desenhar uma arquitectura de gestão que requeresse poucos recursos; as velocidades de transmissão das redes da altura eram baixas e por isso importava escolher um protocolo de transporte da informação de gestão que fosse eficiente e que não utilizasse demasiadamente a capacidade da rede para o transporte de informação de gestão. A simplicidade da sua arquitectura teve dois efeitos curiosos: por um lado levou, ao longo do tempo, a inúmeras acusações acerca das limitações do protocolo, especialmente as relativas à falta de segurança; por outro, levou à massificação da sua utilização não havendo actualmente elemento ou impressora de rede, por mais simples ou complexo que seja, que não implemente suporte de gestão baseada em SNMP.

O modelo de gestão criado assenta na utilização de três componentes: os elementos geridos designados por agentes SNMP; as estações de gestão que gerem os agentes de rede e que segundo a arquitectura cliente - servidor funcionam como clientes; e um protocolo designado de SNMP que define as mensagens, o seu formato e a sua temporização. Cada agente é visto como um conjunto de objectos variáveis que representam informação relativa ao seu estado actual e são disponibilizados para consulta e/ou alteração por parte do gestor. O gestor é responsável pela monitorização, pela geração de relatórios, por efectuar a configuração dos agentes e efectua também a interacção com o gestor humano da gestão da rede. O agente implementa um repositório de informação de gestão designado de *Management Information Base* (MIB), disponibiliza ao gestor acesso à informação de gestão e encarrega-se da notificação de ocorrência de eventos específicos ao elemento gestor.

Em 1992 surgiu uma série de documentos designados por *Secure* SNMP com o objectivo de ultrapassar o problema da segurança do modelo. Estes acabaram por estar na base de uma nova

versão do protocolo SNMP (SNMPv2) que se encontra descrito nos RFCs 1441 a 1452. Estas alterações ao protocolo acabaram por não ter aceitação devido a problemas na sua especificação, sendo em 1996 proposta uma outra versão do protocolo (SNMPv2c) que mantêm intacta a estrutura funcional da arquitectura, mas que elimina a componente da segurança. Em 1998, foi publicada uma série de RFCs, do 2571 ao 2575 que definiram uma forma de acrescentar a segurança e o controlo de acessos às funcionalidades já definidas no SNMPv1 e SNMPv2, criando assim uma nova versão do protocolo designada de SNMPv3.

Apesar de o modelo de gestão SNMP disponibilizar suporte de alteração das variáveis de gestão, provavelmente por questões relacionadas com as deficiências apontadas ao nível de segurança, as implementações de gestão SNMP limitam-se ainda hoje quase exclusivamente a acções de monitorização. Na sua maioria as soluções de gestão utilizam o protocolo SNMP como ferramenta de leitura de informação, e utilizam protocolos por vezes proprietários do fabricante como *Command Line Interface* (CLI) para efectuar as acções de configuração dos elementos de gestão.

O SNMP é um protocolo binário, com um conjunto bastante limitado de mensagens [10]. Utiliza tipicamente o protocolo da camada de transporte UDP como forma de limitar a utilização dos recursos de rede, facto muito importante numa situação em que a rede se encontre sobrecarregada e seja necessária alguma acção de configuração para corrigir o seu mau funcionamento. Pacotes pequenos terão sempre maior probabilidade de conseguir chegar ao destino do que os pacotes maiores. Pequenas quantidades de tráfego gerado permitem a utilização da capacidade de transferência da rede para a sua função de transporte de informação.

A Tabela 2.1 lista o conjunto de mensagens definidas no protocolo SNMP, identifica a sua origem e inclui uma breve descrição do seu significado.

Tabela 2.1 - Conjunto de mensagens definidas no protocolo SNMP.

ENTIDADE	ORIG. ->DEST.	DESCRIÇÃO
Get-request	gestor -> agente	Pede o valor de uma ou mais variáveis
Get-next-request	gestor -> agente	Pede o valor da variável seguinte à corrente, de forma alfabética
Get-bulk-request	gestor -> agente	Pede o valor de toda uma tabela de variáveis
Set-request	gestor -> agente	Actualiza uma ou mais variáveis
Inform-request	gestor -> gestor	Mensagem trocada entre estações de gestão, com o objectivo de descrever uma MIB local
Trap	agente -> gestor	Mensagem enviada dos agentes para as estações de gestão

Uma vez que o gestor funciona maioritariamente como o cliente, seguindo uma filosofia cliente – servidor, a mensagens são na sua maioria enviadas do gestor para o agente. O agente responde com as informações solicitadas ou confirma ao gestor que actualizou o seu estado de acordo com o solicitado. Na ausência de controlo de fluxo de mensagens cabe às aplicações a

implementação de mecanismos de controlo da recepção das mensagens. No caso das mensagens *Trap,* o agente toma o papel de cliente e o gestor o papel de servidor.

Os agentes SNMP armazenam a informação de gestão em *Management Information Base* (MIB). As MIB são repositórios de informação estruturados onde os objectos possuem um nome, uma sintaxe e uma codificação representada em *Abstract Syntax Notation One* (ASN.1). Os objectos são univocamente distinguidos através do seu *Object Identifier* (OID) que são representados na forma de um conjunto de números separados por pontos, onde cada número define um determinado nó da árvore hierárquica (Figura 2.12). A atribuição é feita pelo IAB sendo atribuído a cada nó um determinado número e nome. Por exemplo o identificador *1.3.6.1.1* corresponde a *iso.dod.internet.directory*. Os tipos de dados representáveis numa MIB são definidos pela linguagem ASN.1 e incluem INTEGER, OCTET STRING, OBJECT IDENTIFIER, SEQUENCE, SEQUENCE OF.

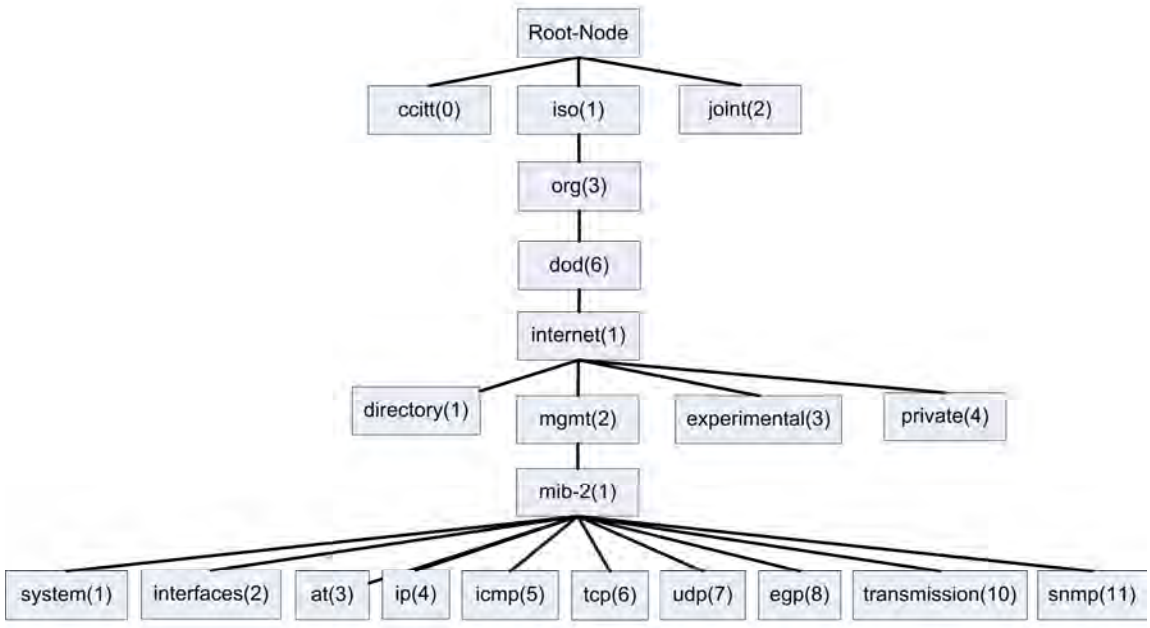

Figura 2.12 – MIB SNMP.

As MIB podem ser definidas pelo IETF (*standard*) ou proprietárias dos fabricantes (enterprise). São exemplos de MIB *standard*: *X.25*, *Modems*, *DS1*, *DS3*, *Bridges*, *ATM*, *Token Ring*, *Ping*, *Traceroute*, *Print Job Monitoring*.

2.3.2 Common Open Policy Service (COPS)

Em Setembro de 1999, o IETF propôs uma arquitectura para uma plataforma de gestão baseada em políticas [11]. Foram propostos os principais componentes mas não foram definidos os

detalhes de implementação como, por exemplo, a plataforma, os protocolos de distribuição de politicas ou a linguagem de definição das mesmas. A arquitectura proposta define um conjunto de entidades de gestão (Figura 2.13): a consola de edição de políticas, o Ponto de Definição de Políticas (PDP- *Policy Definition Point*), o Ponto de Execução de Políticas (PEP – *Policy Enforcement Point*) e ainda um repositório de políticas do sistema.

A consola de edição de políticas constitui o elemento único de interacção com o operador humano. Serve como interface de definição das políticas bem como visualizador de políticas previamente definidas. O PDP serve como decisor do sistema de gestão fazendo a gestão integrada e automática de todos os equipamentos a gerir. Os PEPs recebem as políticas do PDP e aplicam-nas às entidades geridas no sistema. O repositório de políticas armazena as políticas definidas pelo operador humano e fornece-as ao PDP.

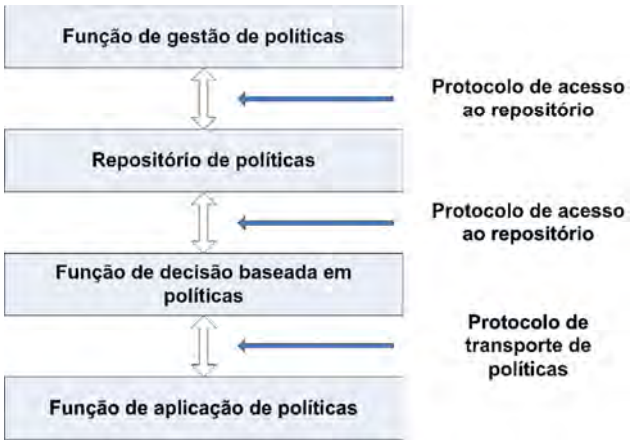

Figura 2.13 - Modelo de referência do Policy Framework do IETF [12].

O protocolo *Common Open Police Service* (COPS) [13] foi desenvolvido pelo grupo de trabalho *Resource Allocation Protocol* (RAP) do IETF, para servir de modelo para a comunicação da informação de políticas entre PDPs e PEPs. Este protocolo baseia-se num modelo cliente/servidor em que o PEP (cliente) envia pedidos ao PDP (servidor) que por sua vez responde enviando decisões ao PEP. Um PDP pode controlar vários PEPs e um PEP pode ser controlado por vários PDPs, apesar de um só PDP ser considerado o PDP principal. A comunicação é feita através da troca de mensagens entre ambas as entidades.

O protocolo COPS apenas define a estrutura das mensagens que transportam os dados, sendo a estrutura dos dados definida para cada tipo de cliente. Utiliza ligações TCP para garantir que as trocas de mensagens entre o servidor e os seus clientes sejam confiáveis. É um protocolo baseado em estados, o que significa que o servidor guarda o estado dos clientes e que pode a qualquer momento alterar a sua configuração, mesmo que não seja solicitado. O COPS tem mecanismos de segurança para autenticação e integridade das mensagens, podendo ainda usar os

protocolos de transporte IPSEC e TLS para autenticação e segurança das comunicações. É um protocolo flexível e extensível, suportando novos tipos de clientes sem ser necessário alterar o protocolo.

Em COPS, ao contrário do que acontece por exemplo com o protocolo SNMP, o PEP estabelece uma ligação TCP única com um PDP, para enviar pedidos e receber decisões ou directivas do PDP.

O protocolo *COPS for Provisioning* (COPS-PR) [14] é uma extensão ao protocolo COPS e foi desenvolvido pelo grupo de trabalho RAP do IETF. Este protocolo suporta o modelo de aprovisionamento para a gestão baseada em políticas, segundo o qual o servidor de políticas (PDP) envia toda a informação necessária para configurar os seus clientes (PEPs). Distingue-se assim do modelo anterior (*Outsourcing*), em que existe um relação directa entre cada pedido do PEP e a correspondente decisão do PDP. A Figura 2.14 ilustra os componentes e o princípio de funcionamento do modelo COPS-PR.

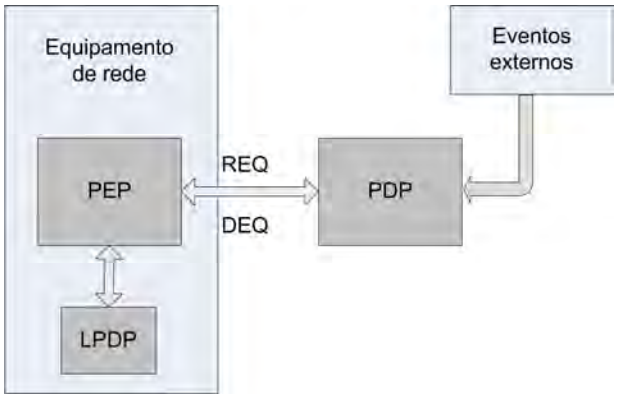

Figura 2.14 - Funcionamento COPS-PR.

Inicialmente o cliente PEP estabelece uma ligação COPS com o seu servidor PDP primário. Seguidamente o PEP envia ao PDP um pedido de configuração, juntamente com a informação que o descreve. O PEP pode também especificar o tamanho máximo da mensagem COPS-PR que suporta. Em resposta o PDP envia, através de uma mensagem de decisão (DEC), as políticas relevantes para o PEP aplicar. Sempre que o PDP detectar alterações das condições envia ao PEP as actualizações das políticas para o PEP instalar. Se entretanto a configuração do dispositivo se alterar tornando as políticas instaladas desadequadas, o PEP pode enviar ao PDP um pedido de actualização da sua configuração acompanhado de informação sobre o seu estado.

O COPS é um protocolo especialmente concebido para comunicar informação de políticas a dispositivos de rede permitindo o controlo de admissão de pedidos de recursos de redes baseados em políticas. *Resource ReserVation Protocol* (RSVP) [15] é um protocolo de sinalização que tem como objectivo a reserva de recursos de rede, para garantir que as aplicações possam transmitir

dados entre uma origem e um destino com uma determinada velocidade e qualidade garantidas. A combinação de COPS com RSVP permite uma gestão centralizada da rede, usando o COPS como forma de reencaminhar as decisões de políticas de controlo dos clientes (PEPs) para os servidores de políticas (PDPs). É possível configurar um *router* para processar todas as mensagens RSVP que lhe chegam de acordo com um conjunto de políticas presentes num servidor de políticas, como ilustra a Figura 2.15.

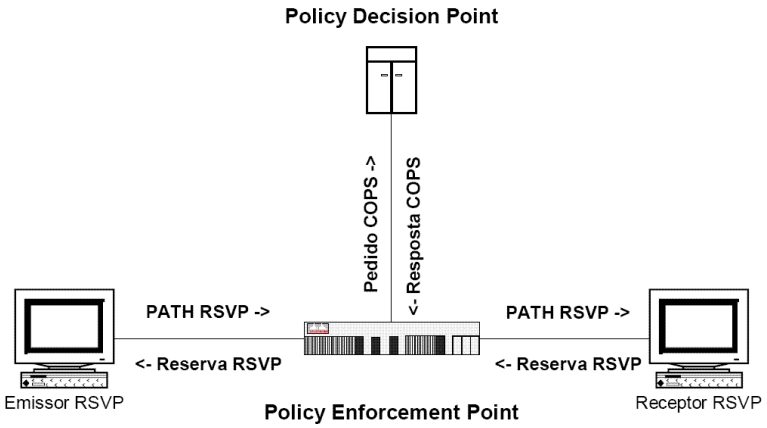

Figura 2.15 - Modelo de funcionamento do COPS-RSVP.

O funcionamento de uma rede como a descrita na figura pode resumir-se nos seguintes passos: assim que é iniciado, o *router* (PEP) tenta ligar-se ao PDP que consta da sua configuração; assim que uma mensagem de sinalização RSVP chega a um PEP, este pergunta ao servidor como processar a mensagem; o servidor, depois de analisar o pedido e consultar a sua lista de políticas, toma uma decisão e responde ao PEP; O PEP ao receber a resposta implementa a decisão enviada pelo PDP. Ao contrário do modelo anteriormente descrito, o modelo COPS-RSVP determina que o PEP não tome nenhuma decisão autonomamente e que exporte todas as decisões para o PDP por si responsável. O modelo COPS-PR confere ao PDP maior autonomia: depois de receber a configuração enviada pelo PDP, o PEP toma todas as decisões de acordo com a configuração previamente recebida.

O protocolo COPS foi concebido de maneira a que as mensagens contenham objectos que se auto identifiquem. Os elementos de policiamento são pedaços de informação necessários para aplicação das regras de policiamento. Os objectos são independentes do protocolo de sinalização de QdS que é usado. As mensagens COPS estão divididas em cabeçalho e objectos.

Em termos de segurança, e ao contrário do protocolo SNMP, são implementados pelo COPS mecanismos de segurança, de forma a garantir a segurança na comunicação entre os elementos do cenário de gestão. As entidades de gestão COPS identificam unívoca das mensagens trocadas e efectuam a troca de chaves de modo a permitir a encriptação das mensagens trocadas.

O modelo de dados utilizado pelos PEPs é designado de *Policy Information Base* (PIB) [16] e permite representar a informação de políticas recebida e armazenada nos PEP. A PIB é representada por uma estrutura em árvore, ilustrada na Figura 2.16, onde os ramos representam tipos de políticas - *Provisioning Classes (*PRC*s)* - e as folhas representam o conteúdo dessas políticas - *Provisioning Instances* (PRIs). Cada ramo da árvore representa as políticas de um determinado tipo, podendo existir várias PRIs para cada PRC. Cada PRI é identificada univocamente pelo *Provisioning Instance Identifier* (PRID) e contém um valor para cada um dos atributos definidos para a PRC da qual é instanciada. Por exemplo, o PRID '1.2.3' representa a PRI '3' da PRC '1.2'. As PIBs seguem a mesma notação e convenções com que se definem as MIBs usadas no protocolo SNMP.

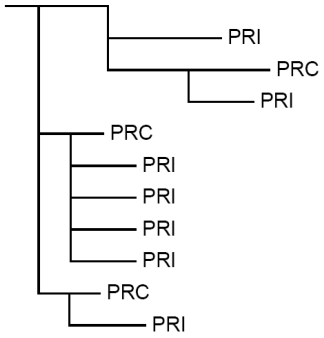

Figura 2.16 - Ilustração da estrutura de uma PIB.

Um PDP pode actualizar (acrescentar, alterar, eliminar) as políticas dos PEP que controla, enviando as regras (PRIs) em mensagens COPS. Para isso o PDP tem que mapear as políticas introduzidas através da consola de gestão nas políticas suportadas pela PIB do PEP.

No COPS-PR as PIBs são especificadas de forma abstracta, sendo os detalhes definidos em documentos separados. As PIBs já existentes cobrem diferentes áreas de gestão, tais como segurança e QdS. Na RFC 3318 são definidas as classes comuns a todas as PIBS existentes ou que venham a ser criadas no futuro. As PIBS são definidas de forma independente dos equipamentos, permitindo que equipamentos diferentes possam ser controlados usando a mesma estrutura de dados e que os PDPs não necessitem de conhecer os detalhes de implementação dos PEPs.

Apesar ser bastante eficiente no transporte de informação, e incluir mecanismos de segurança o protocolo COPS nunca foi encarado como uma alternativa válida ao SNMP. Os fabricantes de equipamentos mantiveram suporte SNMP/CLI até que o próprio IETF deixou de incentivar o desenvolvimento e a utilização do protocolo COPS [17].

2.3.3 Web Based Enterprise Management (WBEM)

A tecnologia *Web Based Enterprise Management* (WBEM) [18] foi inicialmente proposta por um conjunto de empresas entre as quais estavam a Microsoft, a Compaq, a BMC Software, a Cisco Systems e a Intel. O objectivo da iniciativa foi definir uma plataforma de gestão onde todos os sistemas pudessem partilhar a informação de gestão, de uma forma integrada e utilizando as tecnologias existentes tanto quanto possível. Estas empresas, em conjunto com o DMTF, iniciaram a especificação de um modelo independente da tecnologia e dos sistemas operativos.

Como modelo de informação foi utilizado o *Common Information Model* (CIM), um modelo de dados desenvolvido pelo DMTF [19]. A procura de tecnologias implantadas e abertas, conduziu à escolha de algumas tecnologias da Web para a representação e transporte da informação de gestão WBEM: codificação dos objectos CIM em *eXtensible Markup Language* (XML) [20] e transporte da informação em *HyperText Transport Protocol* (HTTP) [21]. Essas três tecnologias são, como ilustrado na Figura 2.17, a marca principal da gestão WBEM e representam os objectivos de uma iniciativa de gestão que visava integrar a gestão de duas áreas tradicionalmente separadas: a gestão de redes e a gestão de sistemas.

O modelo de dados CIM representa elementos de gestão de diferentes áreas e permite integrar informação desses elementos num único sistema de gestão. A codificação da informação de gestão em XML permite que o seu acesso seja feito independentemente da arquitectura computacional do sistema bem como do sistema operativo utilizado e ainda que, graças à componente semântica do XML, seja facilmente desenvolvido suporte de gestão por parte de um fabricante de soluções de gestão. Sendo o protocolo HTTP bastante utilizado, o desenvolvimento da componente de comunicação dos elementos de gestão WBEM fica também facilitado.

Figura 2.17 - Tecnologias representativas da gestão WBEM.

Grande parte das empresas pertencentes ao grupo propulsor da iniciativa WBEM promoveu posteriormente projectos de desenvolvimento em regime de código aberto, de soluções de gestão

baseadas em tecnologia WBEM. São bons exemplos OpenPegasus [22], OpenWBEM [23], SBLIM [24], WBEM Services [25] e SNIA CIMOM [26]. Foram também criados vários produtos comerciais de gestão baseados nesta tecnologia: Tivoli da IBM, CiscoWorks2000, Solaris WBEM service da Sun e HP WBEM SDK da HP. A Microsoft criou uma implementação da norma de gestão WBEM que baptizou de *Windows Management Instrumentation* (WMI) [27]. A maioria dos seus sistemas operativos disponibilizam suporte WMI e a Microsoft fornece também soluções comerciais de gestão como o *Microsoft Operations Management.*

As implementações WBEM são maioritariamente interoperáveis entre si, inclusivamente a implementação WBEM da Microsoft, graças às tecnologias de base utilizadas. Em [28, 29] são efectuadas comparações entre as iniciativas de desenvolvimento em regime de código aberto das plataformas de gestão WBEM.

A arquitectura típica de uma plataforma WBEM, inclui 5 elementos (Figura 2.18): o *CIM Object Manager* (CIMOM), o repositório, os adaptadores (WBEM *providers)*, os elementos geridos e uma consola de gestão. O CIMOM é o elemento central na plataforma de gestão: constitui o elemento central de gestão, comunica através dos adaptadores com as entidades geridas e recebe informação de configuração do operador humano através da consola de gestão. Mantém ainda a informação de gestão no repositório de dados que pode consultar sempre que necessite.

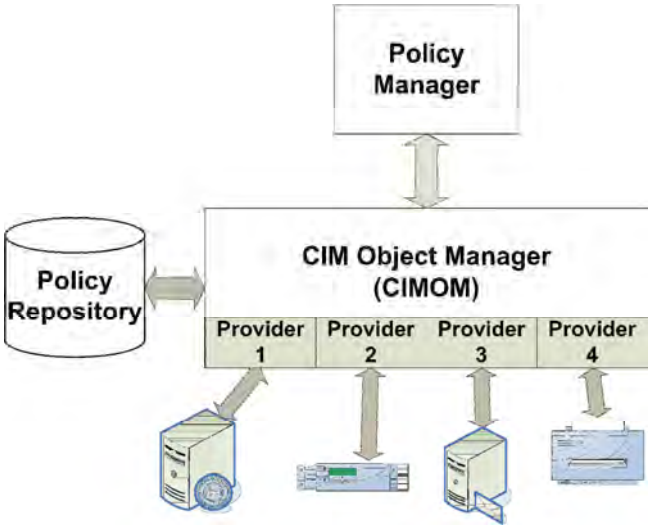

Figura 2.18 - Arquitectura típica WBEM.

Os adaptadores estabelecem a comunicação entre os elementos geridos e o CIMOM, tipicamente implementados como extensões funcionais do CIMOM, inclusivamente, na maior parte dos casos, são implementados como bibliotecas dinâmicas que são carregadas pelo processo do CIMOM. Atendendo ao carácter generalista das acções de gestão implementadas pelo CIMOM, cabe aos adaptadores implementar as funcionalidades específicas inerentes às características

particulares dos objectos CIM criados como extensões ao modelo CIM base. Os adaptadores podem ser classificados em quatro grupos:

- adaptadores de instâncias (*instance providers)*, que permitem ao CIMOM configurar as propriedades das diferentes instâncias de gestão de um determinado objecto*;*
- adaptadores de métodos *(method providers)*, que permitem ao CIMOM invocar métodos dos objectos de gestão*;*
- adaptadores de indicações (indication providers), que servem para implementar ferramentas de monitorização permitindo enviar eventos (indicações na nomenclatura CIM [30]) ao CIMOM e os adaptadores de associação (association providers), que implementam e gerem relações entre os objectos CIM;
- adaptadores mistos quando implementam funcionalidades de mais do que um dos tipos de funcionalidades anteriormente listados.

O processo de desenvolvimento de uma solução de gestão WBEM consiste na instalação das aplicações pertencentes à plataforma CIM e na criação dos objectos CIM no servidor. Os objectos CIM são especificados no formato *Managed Object Format* (MOF) [19] e são posteriormente compilados e carregados no servidor. O processo de carga dos objectos definidos no ficheiro MOF pode resultar na criação de novas extensões ao modelo CIM.

O exemplo da Figura 2.19 ilustra a definição de dois objectos derivados de *CIM_LogicalElement*: (o *CIM_System* e o *CIM_LogicalDevice*), bem como a definição de um objecto agregador chamado *CIM_SystemDevice*.

```
class CIM_System:CIM_LogicalElement
{
        [Key]
        string Name;
};
class CIM_LogicalDevice: CIM_LogicalElement
{
        [Key]
        string DeviceID;
        [Key, Propagated("CIM_System.Name")]
        string SystemName;
};

[Association]
class CIM_SystemDevice: CIM_SystemComponent
{
        [Override ("GroupComponent"), Aggregate, Min(1), Max(1)]
        CIM_System Ref GroupComponent;
        [Override ("PartComponent"), Weak]
        CIM_LogicalDevice Ref PartComponent;
};
```

Figura 2.19 – Exemplo de ficheiro MOF.

O protocolo de comunicação entre elementos de uma plataforma WBEM é CIM-XML em HTTP [21]. Foi definido com o intuito de maximizar a interoperabilidade das soluções de gestão,

bem como disponibilizar uma norma aberta de fácil implementação por parte dos fabricantes. Utiliza mensagens HTTP, tipicamente nos portos 5988 (HTTP) e 5989 (HTTPS), tanto TCP como UDP.

As mensagens definidas pelo protocolo incluem pedidos implementados através de mensagens *HTTP Post*, enquanto as mensagens de resposta são transportadas em mensagens *HTTP Response*. Os pedidos são ainda diferenciados entre: operações intrínsecas CIM, que são mensagens usadas para invocar uma operação sobre um *namespace*; e mensagens de exportação CIM, como as mensagens de comunicação acerca de objectos CIM externos ao *namespace*. A norma define um conjunto de operações intrínsecas, listadas na Tabela 2.2, que permitem aos elementos de gestão manipular remotamente os diversos objectos CIM. Permitem acções de leitura e de escrita sobre os objectos CIM com diferentes granularidades, desde o *namespace* até à propriedade.

Tabela 2.2 - Operações intrínsecas definidas pela norma CIM [21].

ÂMBITO	FUNCIONALIDADE BÁSICA	OPERAÇÃO
Schema	Leitura de qualificadores	EnumerateQualifiers
		GetQualifier
	Escrita de qualificadores	SetQualifier
		DeleteQualifier
Namespace	Leitura	EnumerateClasses
		EnumerateClassName
	Leitura e escrita	ExecQuery
Classe	Leitura	GetClass
	Escrita	CreateClass
		ModifyClass
		DeleteClass
Associações	Leitura	Associators
		AssociatorNames
		References
		ReferenceNames
Instância	Leitura	GetInstance
		EnumerateInstances
		EnumerateInstanceName
	Escrita	CreateInstance
		ModifyInstance
		DeleteInstance
Propriedade	Leitura	GetProperty
	Escrita	SetProperty
Adaptador	Invocação de método	InvokeMethod

Os pedidos, tal como os objectos, são codificados em XML. A Figura 2.20 ilustra um pedido de um cliente CIM para que seja executada uma query CIM Query Language (CQL) [31] (*SELECT * FROM D_Interface*). No pedido são definidos a versão da especificação, a codificação utilizada na mensagem HTTP, o tipo de operação CIM invocada, o *namespace* sobre o qual a instrução WQL devia ser executada e o tamanho da mensagem HTTP que transporta o pedido.

```
POST http://192.168.2.4:5988/cimom HTTP/1.1Authorization: Basic cm9vdDpxd2VydHk=Host:
192.168.2.4:5988 Pragma: no-cache Proxy-Connection: Keep-Alive Content-type:
application/xml; charset="utf-8" CIMProtocolVersion: 1.0 CIMOperation: MethodCall
CIMMethod: ExecQuery CIMObject: root%2Fcimv2 Content-Length: 476

<?xml version="1.0" encoding="utf-8" ?><CIM CIMVERSION="2.0" DTDVERSION="2.0"><MESSAGE
ID="4711" PROTOCOLVERSION="1.0"><SIMPLEREQ><IMETHODCALL
NAME="ExecQuery"><LOCALNAMESPACEPATH><NAMESPACE NAME="root"></NAMESPACE><NAMESPACE
NAME="cimv2"></NAMESPACE></LOCALNAMESPACEPATH><IPARAMVALUE NAME="QueryLanguage"><VALUE>WQL
</VALUE></IPARAMVALUE><IPARAMVALUE NAME="Query"><VALUE>select * from D_Interface</VALUE>
</IPARAMVALUE></IMETHODCALL> </SIMPLEREQ></MESSAGE></CIM>
```

Figura 2.20 – Exemplo de pedido ExecQuery de CIM-XML em HTTP.

Common Information Model (CIM) [32] é um modelo de dados orientado a objectos onde são representados os dados, os interfaces dos objectos geridos e as relações entre os objectos a gerir. O modelo, como ilustrado na Figura 2.21, é composto por três camadas: *Core Model*, o *Common Model* e o *Extensions Schemas*.

O *Core Model*, representado como um círculo no centro da Figura 2.21, é constituído por um conjunto de associações e de classes abstractas que modelam as características genéricas e comuns a todas as áreas de gestão. Os sistemas, as aplicações e as redes são modeladas como extensões ao *Core Model*.

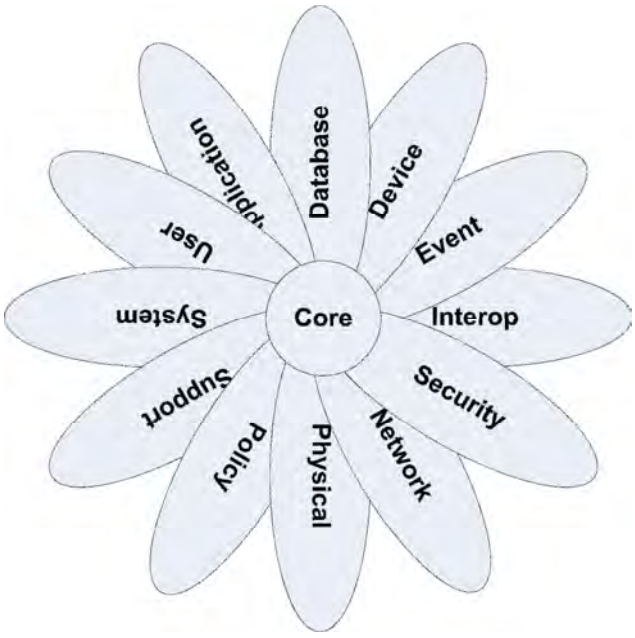

Figura 2.21- Camadas do modelo CIM.

O *Common Model*, representado como elipses na Figura 2.21, é um conjunto de modelos de informação relacionados com áreas específicas de gestão, mas de uma forma independente das tecnologias ou implementações. São exemplos de *Common Models* constantes na versão 2.20.2 do

Schema CIM: *CIM_Application, CIM_Application-J2eeAppServer, CIM_Database, CIM_Device, CIM_Event, CIM_Interop, CIM_IPsecPolicy, CIM_Metrics, CIM_Network, CIM_Physical, CIM_Policy, CIM_Security, CIM_Support, CIM_System e CIM_User*.

A camada *Extension Schema*, que não se encontra representada na Figura 2.21, é constituída por extensões às classes do *Comon Model,* de forma a representar os detalhes específicos de uma determinada tecnologia ou fabricante.

O modelo de eventos CIM (Figura 2.22) define as classes representativas dos eventos pertencentes ao modelo CIM [30], descrevendo a hierarquia de classes descendentes da classe *CIM_Indication* que representam um evento em CIM, bem como as classes derivadas de *CIM_Subcription* que representam subscrições para que se recebam eventos.

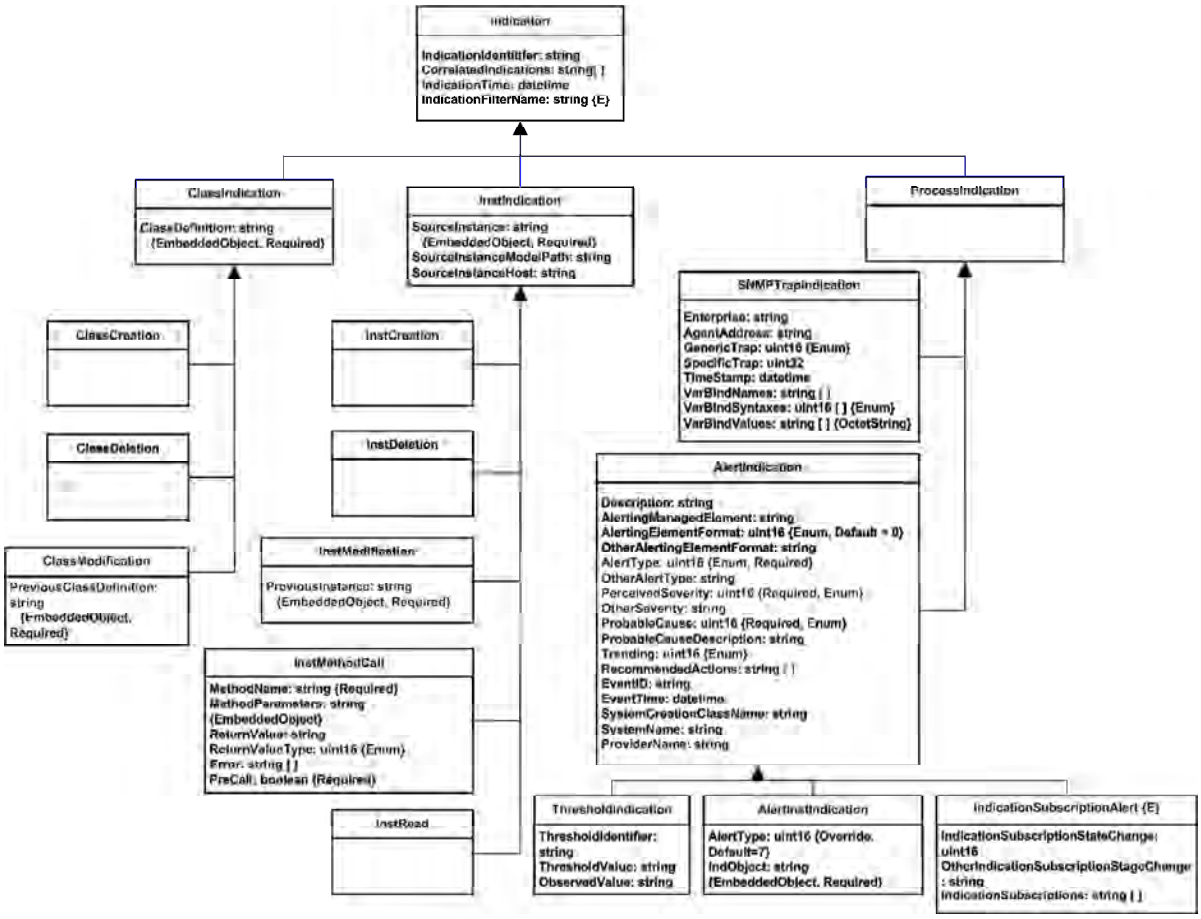

Figura 2.22 - Eventos CIM.

Em CIM os eventos são representados como instâncias das classes derivadas da classe abstracta *CIM_Indication*. Da classe *CIM_Indication* são derivadas 3 classes: *CIM_ClassIndication*, que representa eventos de alteração de uma classe, *CIM_InstIndication*, que representa eventos de alteração de uma instância de uma classe, e *CIM_ProcessIndication*, que

representa um evento de alteração de um processo ou de uma grandeza. Da classe *CIM_InstIndication* são derivadas classes que representam eventos de criação, remoção, modificação, leitura ou invocação de um método de uma instância. Da classe *CIM_ProcessIndication* são derivadas as classes *CIM_SNMPTrapIndication*, que representam eventos criados por mensagens de TRAP SNMP e *CIM_AlertIndication*, que representam eventos de alerta e é derivada, por sua vez, em *CIM_ThresholdIndication*, *CIM_AlertInstIndication* e *CIM_IndicationSubscriptionAlert*.

Os eventos gerados, qualquer que seja o seu tipo, são enviados a uma entidade gestora de eventos que se encarrega de os reencaminhar às entidades consumidoras de eventos. O processo ilustrado na Figura 2.23 desenrola-se em duas fases. Inicialmente as entidades consumidoras de eventos efectuam a subscrição dos eventos junto do gestor de eventos. O processo gestor de eventos, por sua vez, regista a entidade e o respectivo evento.

Numa segunda fase, quando o adaptador de indicações encarregue de monitorizar uma determinada grandeza decide gerar um evento, entrega-o ao gestor de eventos da plataforma de gestão. Quando o evento é recebido pelo gestor, este consulta o seu repositório interno procurando as entidades registadas para receber a notificação da ocorrência do evento, e procede ao respectivo envio.

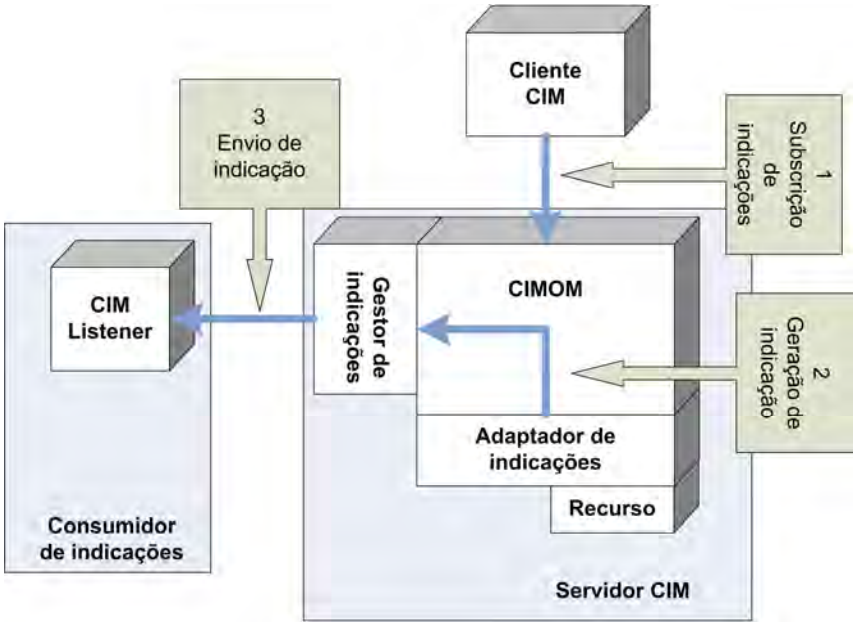

Figura 2.23 – Modelo de gestão de eventos CIM.

A subscrição dos eventos é representada pela classe de associação *CIM_IndicationSubscription*, ilustrada na Figura 2.24, que agrega um objecto da classe *CIM_IndicationFilter* com um objecto da classe *CIM_ListenerDestination*. A classe de associação

CIM_IndicationSubscription armazena informação relativa ao tempo de vida da subscrição, bem como informação relativa à acção a tomar no caso de eventos do mesmo tipo se repetirem várias vezes em pequenos intervalos de tempo. A classe *CIM_IndicationFilter* representa o tipo de eventos que se pretende subscrever através da definição do *namespace* e de uma expressão, tipicamente escrita na linguagem CQL, onde se define o tipo de eventos que se pretende receber. A classe *CIM_ListenerDestination* representa a informação da entidade consumidora dos eventos, contendo os dados relativos ao nome e endereço da mesma.

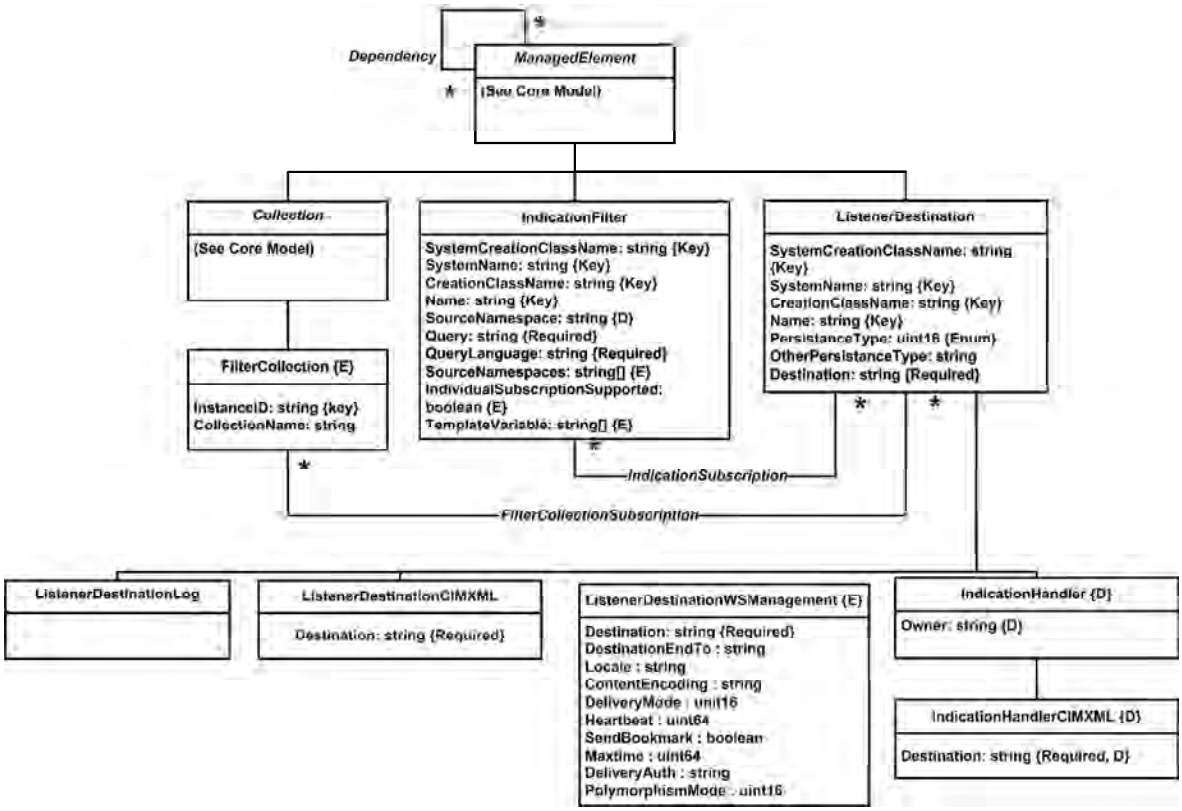

Figura 2.24 - Subscrições CIM.

O modelo de políticas do CIM consiste num conjunto hierárquico de classes extensível para a representação de objectos de políticas [33]. Foi significativamente influenciado pelo modelo PCIM do *IETF Policy Framework Working Group* [34], que por sua vez tinha também sido desenvolvido em estreita ligação com o DMTF e com base na versão 2.2 do CIM Schema.

Cada política é representada como um conjunto de acções e de condições. As condições associadas a uma regra especificam o momento em que é aplicável. As condições podem ser combinadas de duas formas: na forma *Disjunctive Normal Form* (DNF); ou na forma *Conjunctive Normal Form* (CNF). As expressões condicionais podem também ser negadas individualmente. Se a expressão composta for avaliada como verdadeira será executado o conjunto de acções que se

encontra associado à política. É possível definir uma ordem de execução para as acções e indicar se essa ordem deve ser estritamente respeitada ou se é somente indicativa.

O modelo, ilustrado na Figura 2.25, tem como base as classes *CIM_PolicyRule, CIM_PolicyCondition* e *CIM_PolicyAction*, representando os componentes principais de uma política. A classe *CIM_PolicyTimePeriodCondition* permite efectuar a definição do tempo de validade de uma política. As políticas podem ser compostas com outras políticas através da utilização da classe *CIM_PolicyGroup,* facilitando a organização das políticas num servidor. Os grupos de políticas podem incluir outros grupos, permitindo assim representar na hierarquia das políticas a hierarquia existente no cenário de gestão. As políticas podem também receber uma prioridade específica, permitindo por exemplo efectuar a definição de uma regra geral com um conjunto subsequente de excepções. Numa implementação típica as regras são definidas como instâncias das classes *CIM_PolicyGroup, CIM_PolicyRule* e *CIM_PolicyTimePeriodCondition* e como instâncias de classes derivadas de *CIM_VendorPolicyCondition* e *CIM_VendorPolicyAction*.

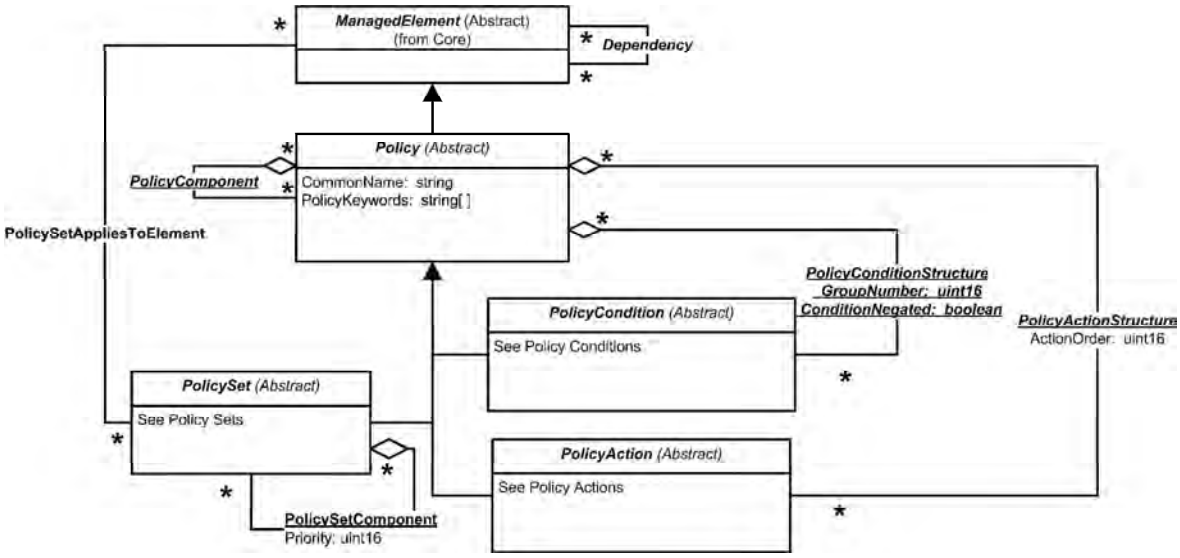

Figura 2.25 - Representação de políticas em CIM.

2.3.4 Directory Enabled Networks (DEN)

O modelo *Directory Enabled Networks* (DEN) [10] resulta de uma iniciativa conjunta da Cisco e da Microsoft, tendo sido posteriormente dinamizada pelo DMTF. O DEN inclui um mapeamento do esquema e do modelo de informação para serviços de directórios que suportem o protocolo *Lightweight Directory Access Protocol* (LDAP) ou outro protocolo de acesso baseado na norma X.500. O mapeamento é uma extensão do CIM, igualmente desenvolvido dentro do DMTF.

O esquema representa o estado persistente dos objectos enquanto que o modelo de informação descreve as relações entre os objectos. Para comunicar com os elementos de rede podem ser usados protocolos como SNMP. A sua implementação permite não só associar serviços a utilizadores e aplicações, como também controlar e configurar os dispositivos de rede de acordo com as suas necessidades. A rede pode ser reconfigurada dinamicamente de acordo com regras representadas no modelo, facilitando a gestão da rede baseada em políticas.

A arquitectura de uma plataforma de gestão baseada no paradigma de gestão DEN é ilustrada pela Figura 2.26. A arquitectura inclui cinco tipos de componentes:

- uma consola de administração;
- um ponto de administração de políticas;
- um repositório constituído por um servidor de directório compatível com DEN onde é armazenada informação sobre políticas e outros dados com elas relacionados (*e.g.:* perfis de utilizadores);
- os PDPs, sendo que existe pelo menos um por domínio administrativo;
- os vários PEPs que existem por domínio administrativo.

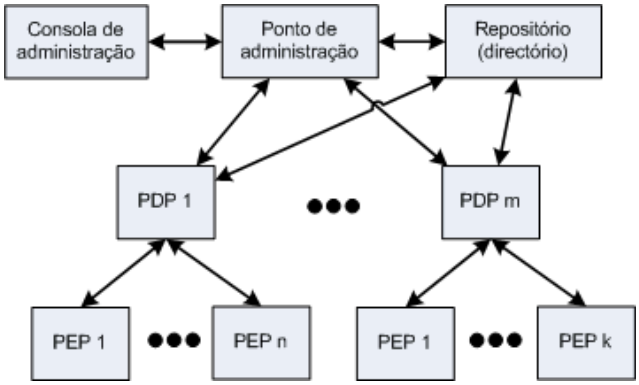

Figura 2.26 - Arquitectura do modelo de gestão DEN.

Um serviço de directório consiste num repositório com informação de recursos organizados hierarquicamente. Os recursos podem ser utilizadores, máquinas, aplicações, serviços, etc. Um serviço de directório tradicional deve ser capaz de armazenar, localizar e identificar qualquer tipo de objectos de forma descentralizada.

A comunicação entre elementos de gestão baseados em tecnologia DEN é feita através do protocolo *Ligthweight Directory Access Protocol* (LDAP) [35]. O LDAP funciona segundo uma arquitectura cliente-servidor, em que os clientes se ligam a um ou mais servidores para actualizarem e obterem informação do directório. Para manipular a informação são definidas várias primitivas, tais como *bind, search, modify, delete*. O protocolo possui um mecanismo que permite aos clientes LDAP passar pesquisas baseadas em texto para servidores LDAP, através da rede.

Quando o servidor não conhece a resposta a uma pergunta do cliente, pode indicar um outro servidor, chamado *referral*, ou uma lista de servidores para o cliente consultar.

Os servidores LDAP são optimizados para operações de leitura e pesquisa, apresentando fraco desempenho em operações de actualização, inserção ou eliminação. Por este motivo, o directório é o tipo de repositório adequado para representar objectos com um tempo de vida longo e propriedades pouco voláteis. É utilizado em vários serviços de directório de diversos fabricantes, tais como o e-Directory da Novell, o Active Directory da Microsoft ou o I-Planet da Sun/Netscape.

O modelo de dados do DEN resulta da junção de conceitos de diferentes versões: da versão 2.0 da especificação do CIM, da especificação X.500 e de um conjunto de novas ideias destinadas a modelar elementos de rede e serviços.

O esquema DEN consiste num conjunto de classes base abstractas a partir das quais todas as outras são derivadas. As classes base são refinadas por especialização do modelo base, para representar elementos de rede, serviços, utilizadores, etc. O esquema base é mostrado na Figura 2.27, com as classes chave do CIM, do X.500 e do DEN, separadas.

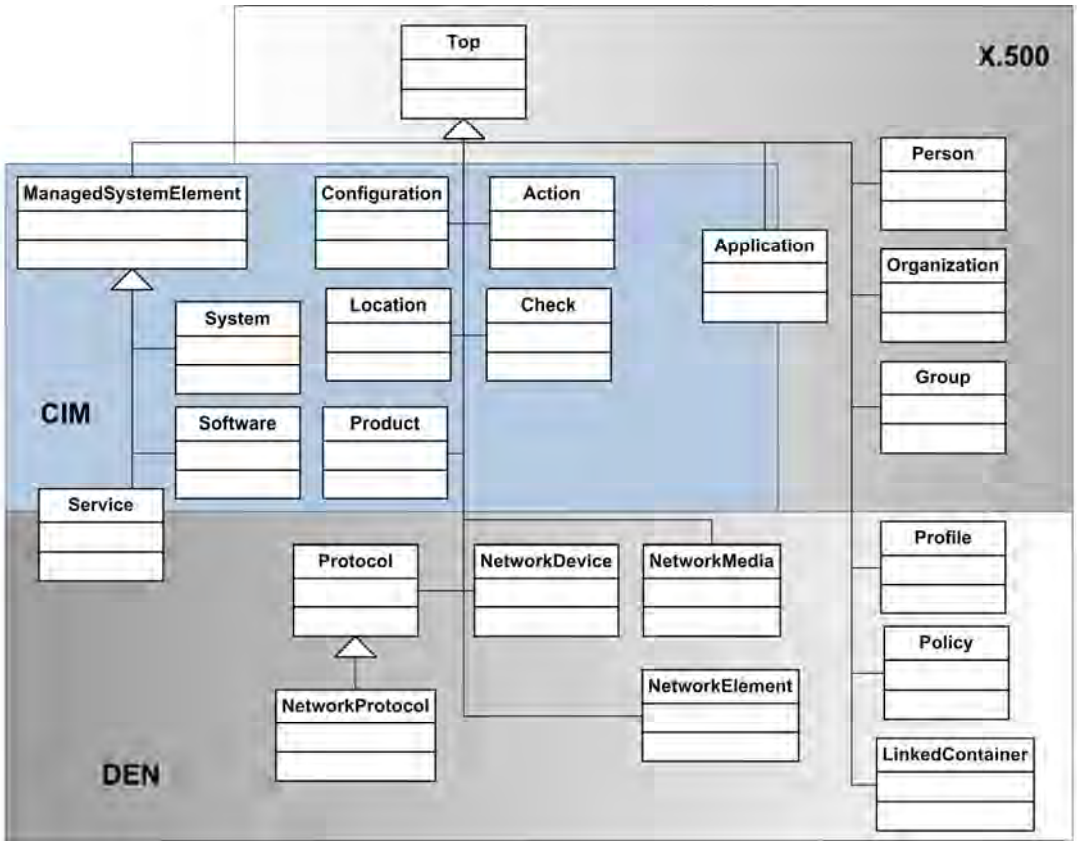

Figura 2.27 - Classes base do DEN.

O protocolo X.500 [36] foi inicialmente publicado em 1988 pelo CCITT, definindo um conjunto de normas que especificam a estrutura de um directório distribuído, baseado numa

estrutura hierárquica de objectos. Os objectos podem ser visualizados e pesquisados por campos arbitrários. O X.500 abrange além de um espaço de nomes, um protocolo de acesso – o DAP, que define a comunicação entre o cliente e o servidor do directório. Pode ser utilizado qualquer cliente X.500 para percorrer o directório, da mesma forma que se utiliza um browser para percorrer a Web.

A informação do directório é armazenada na *Directory Information Base* (DIB) onde cada entrada corresponde a um objecto. Os objectos são organizados numa estrutura hierárquica em forma de árvore. Os objectos que contêm outros objectos são designados por *containers*, os que não contêm são chamados *leaf*. Os objectos são identificados por nomes, que podem ser de dois tipos: o *Relative Distinguished Name* (RDN), que identifica o objecto através de um atributo (ex: cn=pedro) e o Distinguished Name (DN), que identifica o objecto pelo seu nome completo a partir da raiz (ex: cn=pedro,ou=funcionários,o=ua.pt).

A especificação X.500 fornece os seguintes conceitos para o DEN: *Top* para raiz da árvore do directório; *Person* para representar clientes, donos ou administradores; *Group* para representar grupos de utilizadores ou dispositivos; *Organization* para representar entidades de negócio; *Application* para representar o conceito de aplicação; *Directory Server Agent* (DSA) para a própria operação do directório.

A especificação CIM fornece os seguintes conceitos para o DEN: *Product*, *FRU*, etc. que representam produtos e as partes substituíveis de produtos; a classe *ManagedSystemElement* representa qualquer componente do sistema que possa ser gerida e tem como classes derivadas as classes *PhysicalElement* e *LogicalElement*; a classe *Configuration* que representa o comportamento ou estado desejável de um objecto gerido; a classe *Service* para configurar e gerir a implementação de uma funcionalidade; a classe *System* que representa um sistema; a classe *Location* que representa a localização de um elemento físico; a classe *Check* que representa uma condição ou característica que se espera que seja verdadeira; *Action* representa uma operação responsável pela transição de um elemento de software para o estado seguinte, ou que o remove do seu estado actual; e *Application* que representa uma funcionalidade do negócio.

O DEN define também novos conceitos: o conceito de *Profile* que representa um conjunto de atributos e comportamentos que descrevem um objecto ou um conjunto de objectos, um formato diferente de políticas e o conceito de *NetworkMedia* que é uma classe que associa uma interface com os serviços que nela correm. As políticas em DEN consistem em duas componentes: as condições, que definem o contexto em que a política é aplicada; e as acções que são responsáveis pela manutenção do estado do objecto, ou pela sua transição para um novo estado, consoante as condições se verifiquem ou não.

Uma das vantagens da gestão baseada em DEN tem a ver com a utilização de um único repositório de informação, permitindo a reutilização dessa informação pelas várias aplicações de

gestão. As soluções DEN podem também reconfigurar automaticamente a rede como um todo, com base em regras armazenadas num repositório, sem ser necessário definir regras específicas para cada elemento. Uma outra vantagem tem a ver com a possibilidade de reconfiguração automática da rede com base nos perfis de utilizadores e nos serviços. Em contrapartida, uma das desvantagens do modelo DEN é que os sistemas de directório não são os mais adequados para armazenar informação sujeita a actualizações frequentes. É necessário evitar inconsistências na rede, provocadas por atrasos na propagação de alterações, ou pela replicação para evitar percas de dados devidas a falhas no directório. Além disso, os sistemas de directório não suportam o processamento de transacções, o que também pode causar inconsistência dos dados.

Directory Enabled Networks – Next Generation (DEN-ng)

Apesar de ter sido proposto dentro do DMTF o DEN não obteve grande sucesso, tendo ficado demasiado conotado com a tecnologia de directórios proveniente do sistema de comunicação entre gestor e clientes. Entretanto, o DMTF optou por integrar o modelo de dados DEN com CIM acabando por abandonar esta tecnologia em favor da tecnologia WBEM. Discordando dessa decisão John Strassner [37], um dos criadores do modelo DEN, propõe uma nova versão designada de DEN New Generation (DEN-ng) [1] mais ambiciosa e integrando a gestão de sistemas com a gestão do próprio negócio, amplamente ligada ao *New Generation Operations Systems and Software* (NGOSS) [38] do *TeleManagement Fórum* (TMF).

O modelo DEN-ng [1] é um modelo de informação orientado a objectos que representa processos, os dispositivos de rede, as suas configurações, os serviços que propiciam, os utilizadores desses serviços, as regras de negócio, as políticas, entre outras entidades do sistema a gerir. O sistema de informação deste modelo permite que várias entidades de diferentes vendedores possam operar entre si. Os atributos, as operações e os relacionamentos das entidades a gerir, são definidos de uma forma independente de qualquer tipo de repositório, de programa, ou de protocolo de acesso. A informação descrevendo as entidades do sistema a gerir, pode ser partilhada e reutilizada pelas aplicações de gestão e configuração de redes.

Ao permitir expressar regras de negócio, políticas e processos de uma forma comum e normalizada, torna-se possível alterar a configuração de uma rede em resposta a novas regras de negócio. As regras de negócio definem como o negócio é desenvolvido (*e.g.*: 'Vamos oferecer um serviço de VoIP de nível Platina ao Cliente A com um atraso de transmissão mínimo'). As regras são traduzidas em políticas, que por sua vez controlam a configuração dos dispositivos, num processo desenrolado ao longo de várias camadas e designado de *Policy Continuum* (Figura 2.28**).**

O modelo DEN-ng baseia-se na linguagem *Unified Modeling Language* (UML) [39] que é usada na representação dos modelos de informação e de dados utilizados por fornecedores de

serviços e ambientes empresariais. A descrição UML suporta as necessidades dos vários actores das organizações, permitindo que gestores, analistas, programadores, técnicos de suporte e outros, possam comunicar sem deixar de utilizar os termos e conceitos a que estão habituados para expressar as suas necessidades. O modelo DEN-ng utiliza na sua construção padrões e papéis (roles), que tornam o modelo extensível. Os padrões são estruturas pré-concebidas. Os papéis permitem separar o objecto da sua utilização.

Figura 2.28 - Ilustração do conceito de *Policy Continuum* [1].

O modelo DEN-ng define quatro abstracções para que dispositivos com modelos de programação diferentes possam ser tratados como blocos homogéneos na implementação de serviços: *i)* capacidades (*capabilities*), que permitem abstrair funcionalidades específicas dos fabricantes; *ii)* limitações (*constraints*), que definem que capacidades podem ou não ser usadas; *ii)* o contexto, que define o ambiente em que determinada operação tem lugar; e *iv)* os perfis, que expressam os requisitos iniciais dos dispositivos. Em DEN-ng, os objectos que representam utilizadores, dispositivos, serviços e aplicações, são armazenados num directório, utilizando XML sobre LDAP, automatizando a configuração de equipamentos e a activação de serviços de forma independente dos fabricantes dos equipamentos.

O modelo de dados utilizado em DEN-ng é designado por *Shared Information Data* (SID) [40] e é, tal como o CIM, um modelo de informação onde aplicações diferentes podem partilhar e reutilizar a informação de gestão, porque os atributos têm o mesmo nome e tipo de dados, aumentando assim a interoperabilidade entre as ferramentas de gestão e as entidades geridas. A

configuração de dispositivos, serviços e redes orientada pelas regras do negócio permite uma automatização das acções de configuração desencadeada pelo desenvolvimento de novas acções ao nível da camada do negócio permitindo assim um mais fácil e mais rápido desenvolvimento de novas iniciativas de negócio.

A arquitectura de um sistema de gestão PBNM proposta pelo modelo DEN-ng, inclui os seguintes componentes (Figura 2.29): uma consola editora de políticas que interliga o operador humano com o sistema PBNM, um repositório que armazena políticas e informação relacionada, um *Broker* de políticas que coordena os servidores de políticas e os servidores de políticas que incluem um conjunto de PDPs e PEPs que tomam e aplicam as decisões de políticas. A arquitectura DEN-ng acrescenta à arquitectura do IETF um barramento de comunicações o que permite aumentar o número de PDPs, quer em termos de funções, quer em termos de sub-redes. Também resolve os problemas de sincronização, uma vez que os PDPs podem ser notificados das alterações no repositório. Existem três tipos de detecção de conflitos: (*i*) global, (*ii*) local ou intra-PDP e (*iii*) de vizinhança ou inter-PDP, que acontece quando dois PDPs actuam sobre o mesmo dispositivo e necessitam de se coordenar.

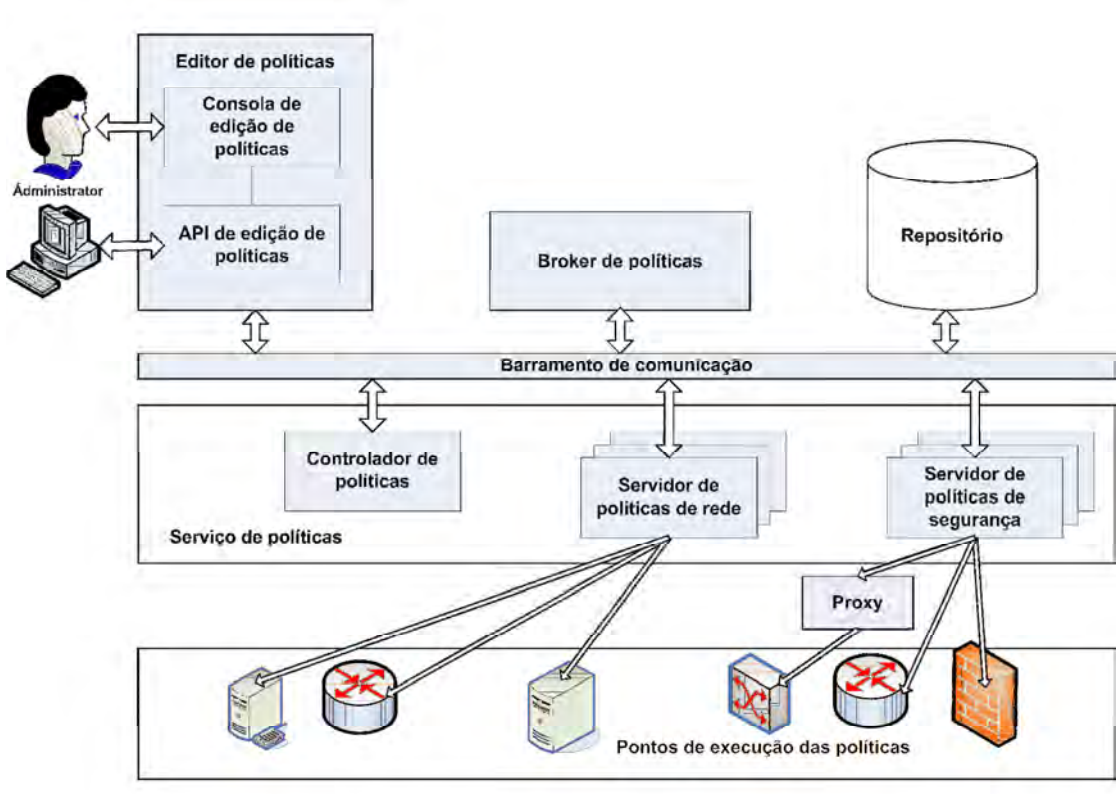

Figura 2.29 - Arquitectura de um sistema baseado no modelo DEN-ng.

2.3.5 Web Services para gestão

A popularidade crescente da tecnologia de sistemas distribuídos baseada em Web Services fez com que se integrasse essa tecnologia nas aplicações de gestão. Foram desenvolvidos esforços de normalização dessas tecnologias preservando a neutralidade em relação aos fabricantes bem como a independência dos protocolos. Em consequência disso foram desenvolvidas duas normas: *Web Services Distributed Management* (WSDM) [41, 42], pela OASIS em 2005, e *Web Services for Management* [43] do DMTF, em 2006. Ambas as especificações utilizam Web Services para a criação de soluções de gestão, especialmente concentradas na gestão de recursos. Fornecem suporte para a criação, remoção e edição de instâncias, suporte para a procura de instâncias bem como suporte de subscrição e notificação de eventos.

A norma WSDM encontra-se dividida em duas componentes: *Management Using Web Services* (MUWS) [41] e *Management Of Web Services* (MOWS) [44]. MUWS concentra-se no fornecimento de uma camada superior que unifique os modelos de gestão existentes enquanto MOWS apresenta um modelo onde o *Web Service* é um elemento gerido. MUWS utiliza um número de especificações como o *Schema* XML, o *Web Services Description Language* (WSDL) [45], bem como um conjunto de especificações temáticas com uma organização semelhante ao *Common Model* do CIM: *Web Services Addressing* (*WS-Addressing*), *Web Services Resource* (*WS-Resource*), *Web Services Notification* (*WS-BaseNotification*), e *Web Services Security* (*WS-Security*).

A iniciativa *Web Services for Management (WS-Management)* define um conjunto de operações disponíveis (Tabela 2.3) para a gestão dos sistemas, divididas em três grupos: grupo de acesso a recursos, o grupo de enumeração, e grupo de gestão de eventos.

Tabela 2.3 - Operações de WS-Management.

ÂMBITO	MENSAGEM	DESCRIÇÃO
Acesso a recursos	Get	Obtêm instâncias de objectos
	Delete	Apaga instâncias de objectos
	Create	Cria instâncias de objectos
	Put	Actualiza informação relativa a uma instância de um objecto
Enumeração	Enumerate	Estabelece um contexto de enumeração
	Pull	Itera através de conjunto de resultados
	Release	Liberta iterador, bem como os resultados associados
Eventos	Subscribe	Subscreve determinados eventos para um cliente
	Unsubscribe	Anula uma subscrição
	Renew	Renova uma subscrição
	SubscriptionEnd	
	Acknowledge of delivery	Confirma recepção de entrega de notificação
	Refusal of Delivery	Recusa entrega de notificação

A maior diferença entre as especificações MUWS e WS-Management está relacionada com a flexibilidade: a primeira disponibiliza uma plataforma mais rica, mais poderosa, com maior diversidade de tipos de dados; a segunda disponibiliza uma especificação mais leve que inclusivamente, segundo Pavlou [46], obtém melhores resultados em termos de desempenho.

Tal como acontece em relação a outras tecnologias baseadas em XML, as mensagens trocadas, têm tamanhos consideráveis devido ao carácter textual da linguagem. A Figura 2.30 ilustra um pedido trocado entre duas entidades de gestão segundo a norma WS-Management.

```
POST /wsman HTTP/1.1
Authorization: Basic cm9vdDpxd2VydHk=
Host: 192.168.2.2:8889
Accept: */*
Content-Type: application/soap+xml;charset=UTF-8
User-Agent: openwsman 2.0.0b1
Content-Length: 1042
Expect: 100-continue

<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd"
xmlns:wsen="http://schemas.xmlsoap.org/ws/2004/09/enumeration"><s:Header><wsa:Action
s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/09/enumeration/Enumerate</wsa:Ac
tion><wsa:To
s:mustUnderstand="true">http://192.168.2.2:8889/wsman</wsa:To><wsman:ResourceURI
s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/*</wsman:ResourceURI><wsa:Mess
ageID s:mustUnderstand="true">uuid:f093afbe-4a70-1a70-8002-
e675dd8f1300</wsa:MessageID><wsa:ReplyTo><wsa:Address>http://schemas.xmlsoap.org/ws/2004/08
/addressing/role/anonymous</wsa:Address></wsa:ReplyTo></s:Header><s:Body><wsen:Enumerate><w
sman:OptimizeEnumeration/><wsman:Filter
Dialect="http://schemas.microsoft.com/wbem/wsman/1/WQL">select * from
D_Interface</wsman:Filter><wsman:MaxElements>10</wsman:MaxElements></wsen:Enumerate></s:Bod
y></s:Envelope>
HTTP/1.1
```

Figura 2.30 – Exemplo de pedido WS-Management.

A norma WS-Management utiliza o modelo de dados CIM para a representação de informação [47, 48], tal como a tecnologia WBEM anteriormente desenvolvida pelo DMTF.

2.3.6 Diameter

O protocolo Diameter nasceu como um substituto para o protocolo *Remote Authentication Dial In User Service* (RADIUS) [49] tipicamente utilizado em serviços de autenticação, autorização, registo e contabilização (AAAC), para ligações ponto a ponto e para acesso a terminais remotos. O desenvolvimento do protocolo Diameter ocorreu mantendo o formato básico do RADIUS e tentando eliminar algumas deficiências já conhecidas. Apesar das alterações introduzidas neste novo protocolo, o Diameter mantém a compatibilidade com o RADIUS em vários pontos da sua arquitectura, como por exemplo no formato dos *Attribute-Value Pair* (AVP) e

na numeração dos *Command-Code*. Esta compatibilidade permite aos servidores Diameter facilmente mapearem os atributos RADIUS para os AVPs Diameter.

A ideia que esteve na base do Diameter foi a criação um protocolo base que pudesse ser genericamente estendido a novos métodos de acesso. O Diameter consiste num protocolo base [50] com diferentes extensões e aplicações como ilustra a Figura 2.31: *Cryptographic Message Syntax-Security (*CMS-Security*)*, *Network Access Server REQuirements* (NASREQ) e *Mobile-IP*. As funcionalidades básicas comuns a todas as aplicações e serviços são implementadas no protocolo base, enquanto que todas as funcionalidades específicas existem dentro das extensões. O protocolo base dispõe de capacidade de negociação da forma como as mensagens são enviadas. Define também regras que são aplicadas a todas as trocas de mensagens entre nós Diameter e especifica como deve ser a formatação e o transporte das mensagens. Outra função é reportar erros e definir serviços de segurança para serem utilizados por todas as aplicações devendo ser suportados por todas as implementações Diameter.

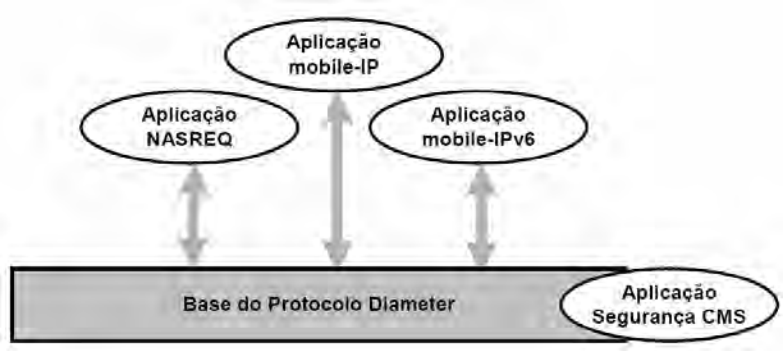

Figura 2.31 - Arquitectura de protocolo Diameter.

O protocolo base do Diameter está intimamente ligado ao módulo de segurança CMS, de modo a fornecer segurança a todas as aplicações. Os servidores com outros módulos e diferentes funcionalidades podem ainda utilizar também o protocolo base.

O protocolo Diameter utiliza protocolos de transporte com suporte de sessão tais como TCP ou SCTP e inclui mecanismos de segurança. Segue o modelo cliente/servidor com a excepção de algumas mensagens que são iniciadas pelo servidor. Implementa mecanismos de descoberta dinâmica de parceiros e de suporte de negociação de capacidades entre estações.

As mensagens Diameter, tal como as mensagens RADIUS, consistem num cabeçalho (Figura 2.32) seguido de um conjunto de AVPs.

O cabeçalho Diameter contém os seguintes campos: um identificador da versão; um campo (*command-code*) que define o qual o comando da mensagem; um campo (ID da aplicação) para identificar a que aplicações a mensagem se destina a mensagem; um campo (Identificador Nó-a-

Nó) que serve para ajudar a determinar quais as respostas a cada pedido; e um identificador (Identificador entre extremos) que serve para ajudar a detectar mensagens duplicadas.

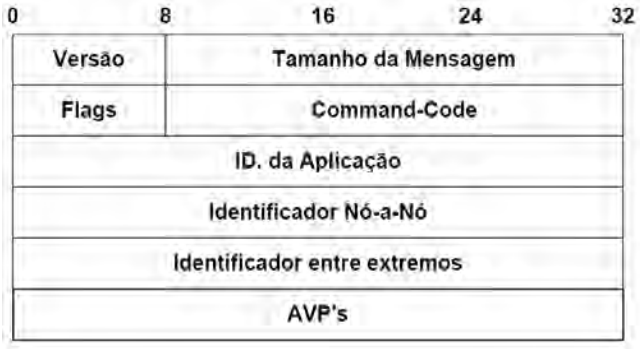

Figura 2.32 – Conteúdo do cabeçalho Diameter.

Cada comando contém um código atribuído, que tanto identifica o pedido como a resposta. A Tabela 8.1 (Anexo A) lista o conjunto de comandos definidos, bem como os respectivos códigos atribuídos.

Os pacotes Diameter incluem depois dos cabeçalhos, objectos designados de AVPs com uma estrutura ilustrada na Figura 2.33. Os AVPs contêm um código identificador, um conjunto de *flags* que indicam ao servidor como tratar dos dados incluídos no AVP, o tamanho do objecto, um campo opcional informando o fabricante e por último os dados contidos no objecto.

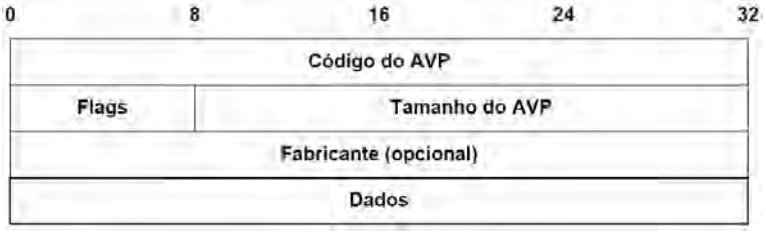

Figura 2.33 - Estrutura de um AVP.

Graças à modularidade da sua arquitectura, têm vindo a ser normalizadas várias aplicações para o protocolo Diameter. Inicialmente as aplicações propostas estavam relacionadas com a gestão de utilizadores e com o funcionamento dos sistemas de autenticação e autorização. Recentemente, com a vasta utilização do protocolo Diameter na arquitectura *IP Multimedia SubSystem* (IMS) do 3GPP, tem vindo a ser proposto um conjunto de extensões para Diameter que incluem: suporte para *Session Initiation Protocol* (SIP) [51], suporte para *Mobile IPv6* (RFC 5447), controlo de admissão baseado em políticas (RFCs 5224 e 5431) e o registo de um conjunto de códigos de comando para utilizar na versão *Evolved Packet System* [52] da plataforma IMS (RFC 5516).

2.3.7 NETCONF

O NETCONF é um protocolo proposto dentro do IETF para a gestão de equipamento de rede heterogéneo. A comunicação implementada pelo NETCONF é baseada em *Remote Procedure Calls* (RPC) codificadas em mensagens XML. Segue o modelo cliente/servidor, sendo o agente de gestão a assumir o papel de servidor. Existem algumas alternativas para o transporte das mensagens NETCONF como os protocolos TCP, *Secure Shell Protocol* (SSH), *Blocks Extensible Exchange Protocol* (BEEP), *Simple Object Access Protocol* (SOAP) ou ainda *Transport Layer Security* (TLS).

O protocolo NETCONF suporta operações de leitura, de edição e de cópia de configuração. Também permite apagar a configuração existente nos agentes e suporta mecanismos de controlo de concorrência no acesso aos elementos de configuração, implementados através da operação de *lock*. A Tabela 2.4 sumaria as operações implementadas pelo protocolo.

Tabela 2.4 - Conjunto de mensagens NETCONF.

OPERAÇÃO	DESCRIÇÃO
<get>	Obtém dados de configuração ou informação acerca do estado do agente
<get-config>	Obtém informação acerca da configuração do agente
<edit-config>	Modifica total ou parcialmente a configuração de um agente.
<copy-config>	Copia a configuração de um agente.
<delete-config>	Remove a configuração de um agente.
<lock>	Bloqueia acesso a elemento de configuração para acesso exclusivo
<unlock>	Liberta bloqueio anterior
<close-session>	Fecha a sessão.
<kill-session>	Para qualquer operação em execução e fecha a sessão
<create-subscription>	Cria subscrição de eventos
<notification>	Envio de notificação

O protocolo foi conceptualmente dividido em quatro camadas (Figura 2.34): os protocolos de aplicação representam os protocolos da camada de aplicação que efectuam o transporte das mensagens NETCONF, fornecendo uma comunicação orientada à ligação, fiável e segura; a camada RPC fornece um mecanismo simples de pedido/resposta utilizando mensagens XML que são transportadas pelos protocolos das camadas inferiores e transportando a informação da camada de operações codificada em XML; e a camada superior designada de conteúdo e que consiste na informação de gestão trocada entre as entidades envolvidas no processo de gestão.

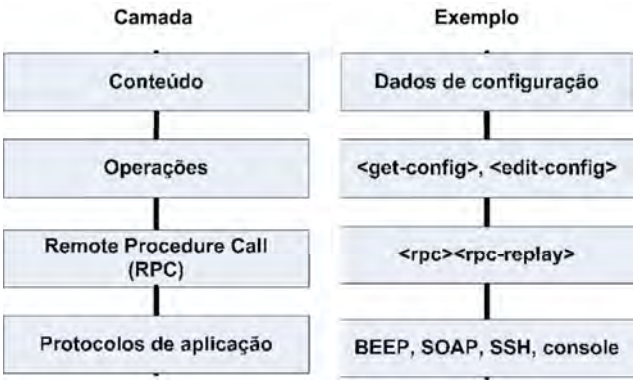

Figura 2.34 - Pilha protocolar do NETCONF.

O modelo de dados a utilizar nas soluções de gestão baseadas em NETCONF não foi ainda definido, apesar de existirem algumas propostas parciais [53]. Têm vindo também a ser propostas várias linguagens de modelação de dados, como XML Schema e *REgular LAnguage for XML Next Generation* (RELAX NG) [54]. Para este efeito, o IETF criou o grupo de trabalho *netmod* com o objectivo de definir uma linguagem amigável para o operador humano, que permitisse definir a semântica dos dados, das operações e das acções de notificação [54].

O grupo *netmod* considerou a linguagem YANG [55], uma linguagem baseada na sintaxe de *Structure of Management Information next generation* (SMIng) [56], como base de trabalho para a definição do modelo de dados do NETCONF.

2.3.8 Modelos de dados conjuntos do IETF e DMTF

Durante os últimos anos tem existido colaboração entre o IETF e o DMTF no sentido de criar modelos de dados específicos para algumas áreas ou até para algumas tecnologias de gestão. A presente subsecção descreve os modelos desenvolvidos conjuntamente pelas duas entidades.

Policy Core Information Model (PCIM)

Policy Core Information Model (PCIM) [57], definido na RFC 3060, é um modelo de informação genérico e orientado a objectos para representar políticas de qualquer tipo, tendo sido desenvolvido conjuntamente pelo IETF e pelo DMTF como uma extensão ao modelo CIM. O modelo define duas hierarquias de classes extensíveis para representar políticas de qualquer tipo: classe estruturais que representam informação de políticas e classes associativas que permitem relacionar as classes estruturais. As extensões ao modelo feitas através da especialização das suas classes permitem representar políticas de áreas específicas. O modelo também suporta a introdução de extensões, de acordo com as necessidades dos fabricantes. A Figura 2.35 mostra de forma genérica as principais classes e relacionamentos do modelo PCIM.

No modelo PCIM uma política consiste num conjunto de regras, cada uma dessas regras consiste num conjunto de condições e de acções. As regras podem ser agregadas em grupos e os grupos podem ser organizados para representar hierarquias de políticas. O modelo permite também definir os períodos em que as regras podem estar activas. Se o valor lógico resultante da avaliação do conjunto de condições associadas a uma regra for verdadeiro, então as acções associadas a essa regra, serão executadas. A sua execução terá como consequência a manutenção do estado do objecto a que são aplicadas, ou a sua transição para um novo estado. É possível especificar a ordem de execução das acções e se a ordem é obrigatória ou apenas recomendada.

Podem ser atribuídas prioridades às regras das políticas e, no caso da aplicação das regras levar à execução de acções contraditórias entre si, serão apenas tidas em conta as acções correspondentes à regra de maior prioridade. As políticas podem existir isoladamente ou agregadas em grupos. Os grupos podem ser constituídos de regras ou de outros grupos, mas nunca de ambos e podem modelar interdependências complexas entre objectos. A agregação de políticas em grupos permite fazer de um grupo de políticas uma unidade reutilizável, podendo ser posteriormente aplicada.

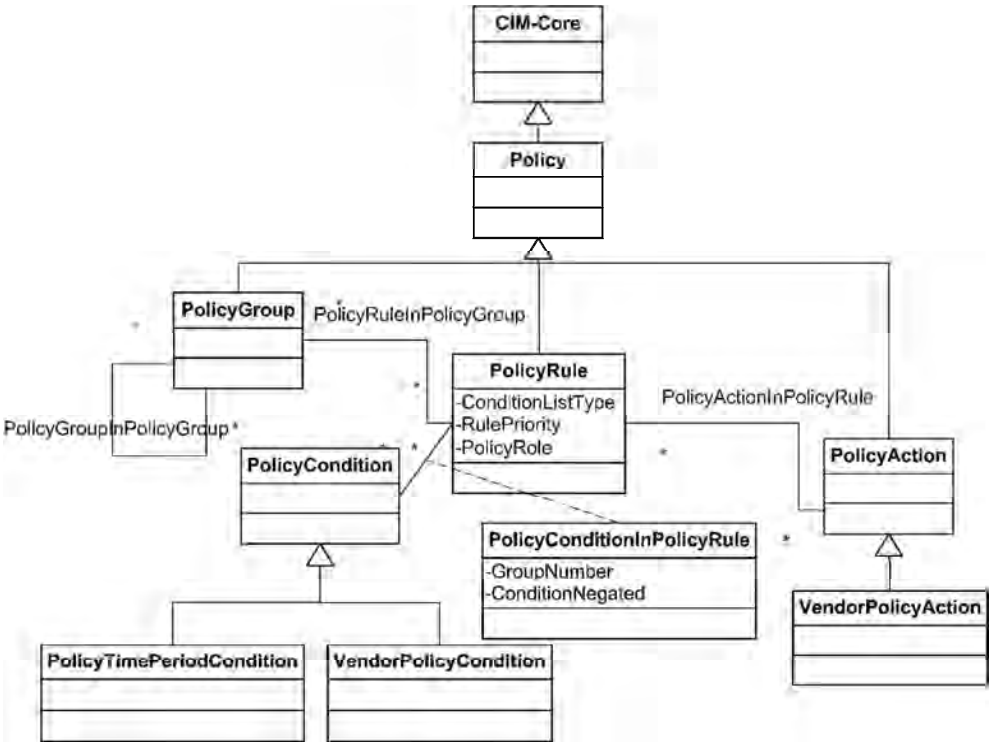

Figura 2.35 - Modelo PCIM.

As políticas podem ser classificadas de acordo com a sua finalidade, nas seguintes categorias: motivação, configuração, instalação, erro, utilização, segurança e serviços. Estas

categorias são representadas no PCIM pelos valores da propriedade *PolicyKeywords* da classe abstracta *Policy*.

Cada recurso pode ser associado a um ou mais papéis (*roles*), sendo definidas políticas para cada um desses papéis. Os recursos são configurados de acordo com os papéis a que estão associados e com as políticas definidas para esses papéis. Deste modo não é necessário configurar cada um dos recursos individualmente. Os papéis podem ser combinados, permitindo aplicar políticas a dispositivos que desempenhem simultaneamente vários papéis, além das políticas correspondentes a cada um dos papéis da combinação. As combinações são representadas no PCIM pelos valores da propriedade *PolicyRoles* da classe *PolicyRule*.

Policy Core Information Model Extensions (PCIMe)

O modelo *Policy Core Information Model Extensions* (PCIMe) [34] introduz alterações ao PCIM que se traduzem na adição de classes para permitir a extensão do modelo a novas áreas e na alteração de alguns elementos do PCIM. As alterações são introduzidas de forma a preservar a interoperabilidade com implementações do modelo PCIM original, que por sua vez segue muito de perto o modelo de políticas CIM do DMTF: podem ser adicionadas novas propriedades às classes existentes; podem ser inseridas novas classes na hierarquia acima das classes existentes sendo que as propriedades das classes existentes podem ser movidas para as novas classes, passando deste modo a ser herdadas em vez de definidas localmente; e que podem ser criadas novas subclasses sendo derivadas a partir das classes existentes.

Policy QoS Information Model (QPIM)

Policy Quality of Service (QoS) *Information Model* (QPIM) [58] é um modelo de informação orientado a objectos que visa a gestão de QdS de serviços diferenciados e serviços integrados, utilizando políticas. O modelo permite especificar e representar políticas de QdS, para administrar, gerir e controlar o acesso a recursos da rede. O QPIM é baseado no modelo PCIM e suas extensões (PCIMe).

O processo de definição de políticas de qualidade de serviço depende de três tipos de informação: as regras de negócio, a topologia da rede e a arquitectura de qualidade de serviço usada na rede. As regras de negócio especificam o comportamento dos vários tipos de tráfego que atravessam a rede. Cada regra define um determinado conjunto de parâmetros do serviço de rede como, por exemplo, a largura de banda, o atraso, a variação do atraso e as perdas de pacotes. O modelo QPIM é usado para ajudar a traduzir as regras de negócio para um formato que expresse os requisitos para o condicionamento dos vários tipos de tráfego da rede. Permite especificar uma funcionalidade de um modo normalizado, independente das capacidades dos dispositivos. O QPIM,

tal como os seus antecessores, usa o conceito de papel (role) para configurar os dispositivos. Os papéis definem as funções dos elementos da rede, independentemente do vendedor e tipo de dispositivo. Isto permite criar políticas para configurar todas as interfaces ou dispositivos que desempenham o mesmo papel, abstraindo dos dispositivos físicos.

As duas arquitecturas de gestão de QdS predominantes são os serviços diferenciados (*DiffServ*) e os serviços integrados (*IntServ*) descritas na subsecção 3.2.1. No suporte incluído no QPIM para a arquitectura de QdS *DiffServ* o QPIM define as condições e acções para controlar classificação, marcação, *metering, dropping, queuing, scheduling, policing e shaping* nas fronteiras do domínio *DiffServ*. No que respeita ao suporte à arquitectura *IntServ*, o QPIM define acções para controlar a reserva de recursos de rede necessária ao estabelecimento de fluxos de pacotes na arquitectura. O QPIM permite que estas arquitecturas possam ser usadas separadamente ou em conjunto.

As acções de QdS são modeladas pelo QPIM, usando as classes *PolicyAction* (definida no modelo CIM), *SimplePolicyAction* (definida no modelo PCIMe) e outras classes derivadas destas, sendo aplicadas ao tráfego seleccionado de acordo com as condições de QdS definidas. A escolha de estruturas hierárquicas para representar políticas assentam em duas razões: em primeiro lugar, porque são as que melhor reflectem a nossa forma de pensar sobre políticas complexas, em segundo lugar, são as que melhor espelham as estruturas administrativas das organizações. Atendendo às heranças que o modelo QPIM teve dos modelos PCIM e CIM, as semelhanças entre os modelos são imensas, pelo que a descrição do modelo de dados será omitida.

Policy Core LDAP Schema (PCLS)

Policy Core LDAP Schema (PCLS) é um modelo desenvolvido pelo IETF [59], que define o modo como é feito o mapeamento das classes estruturais e associativas do PCIM, para o modelo de objectos utilizado pelos serviços de directório baseados no LDAP. No serviço de directório LDAP as classes podem ser abstractas (*abstract*), estruturais (*structural*) ou auxiliares (*auxiliary*). As classes estruturais são as únicas que permitem instanciar objectos. As classes auxiliares possibilitam que os seus atributos sejam adicionados a objectos do directório.

O mapeamento das classes do PCIM em classes do LDAP *Schema,* segue a seguinte estratégia:

- As classes abstractas do modelo PCIM são mapeadas em classes abstractas do LDAP;
- As classes estruturais são mapeadas em três classes LDAP: uma classe abstracta, uma subclasse estrutural e uma subclasse auxiliar;
- As classes associativas podem ser mapeadas de duas formas: em atributos que referenciam *Distinguished Names* (DNs); ou em relacionamentos pai-filho na

Directory Information Tree (DIT). Dois dos atributos que referenciam DNs aparecem em classes auxiliares, o que permite que cada um deles possa representar vários relacionamentos do modelo PCIM.

Para identificar as classes e atributos do LDAP *Schema* é usado o prefixo 'pcim' no nome de cada classe ou atributo PCIM.

QoS Device Datapath Information Model (QDDIM)

QoS Device Datapath Information Model (QDDIM) é um modelo de informação para representar os mecanismos de QdS dos dispositivos de rede [60]. O modelo permite a descrição do condicionamento de tráfego como um conjunto de serviços. Este modelo é influenciado pelo sub modelo *Network QoS* do CIM não derivando de PCIM, apesar de existem ligações com algumas classes do modelo PCIMe. O modelo concentra-se na representação de serviços entre extremos do percurso de dados, focando essencialmente as arquitecturas de *DiffServ* e *IntServ*.

As políticas de QdS representam um *continuum* de especificações que relacionam as regras de negócio com o condicionamento de tráfego realizado pelos dispositivos de rede. A Figura 2.36 apresenta um modelo genérico para este *continuum*.

Figura 2.36 - *Continuum* de políticas QDDIM.

As políticas a nível de negócio expressam os requisitos das aplicações, definindo quais as aplicações que recebem tratamento prioritário quando a rede está congestionada. Ao nível intermédio as políticas de negócio são traduzidas para um conjunto de políticas independentes dos dispositivos, mas dependentes dos mecanismos de QdS, tais como *Random Early Detection*, dropping ou escalonamento *Weighted Round Robin*. A este nível de abstracção é possível gerir vários dispositivos de diferentes capacidades. Ao nível mais baixo encontram-se as políticas dependentes dos dispositivos, que permitem implementar os mecanismos de condicionamento pretendidos.

O modelo QDDIM representa os mecanismos de QdS independentes dos dispositivos. As classes e relacionamentos do modelo representam conceitos abstractos, como é exemplo o 'Serviço Dourado', associando cada um dos serviços aos mecanismos de QdS usados para condicionar o tráfego para esse serviço. O modelo é construído à volta de duas hierarquias de classes ligadas entre si por um conjunto de associações. As duas hierarquias derivam das classes base *QoSService* e *ConditioningService*. A classe *QoSService* é utilizada para representar serviços de rede de alto nível que requerem condicionamento de tráfego. A Figura 2.37 mostra a classe *QoSService* e as suas agregações.

A classe *ConditioningService* representa os mecanismos de condicionamento de tráfego aplicados aos fluxos, primeiro nas interfaces de ingresso e posteriormente nas interfaces de saída dos dispositivos. O modelo define classes para modelar Classificadores, Filtros, Droppers, Filas e Escalonadores. Os relacionamentos são modelados como classes contendo uma referência a cada um dos objectos relacionados. As associações e agregações definidas no QDDIM são binárias, ou seja, são definidas entre duas classes. Não afectam as classes relacionadas, isto é, a criação ou eliminação de uma associação ou agregação, não afecta as interfaces das classes relacionadas.

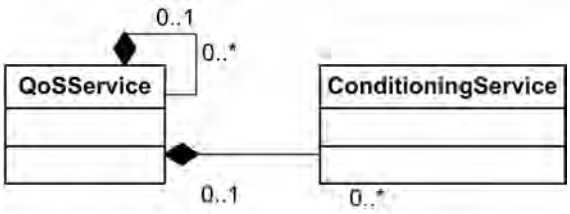

Figura 2.37 - Classe QoSService QDDIM.

2.4 Sumário

Nesta secção foram descritas várias iniciativas de gestão (tecnologias, modelos de dados, protocolos e linguagens de definição de políticas) que foram desenvolvidas desde a introdução do protocolo SNMP no final da década de 80. Estas tecnologias foram maioritariamente desenvolvidas no âmbito do IETF, mas também pelo DMTF onde a perspectiva de desenvolvimento de ferramentas de gestão integrada criou soluções conjuntas, para a gestão de redes e sistemas.

Existe uma tendência de criação de mecanismos de gestão mais poderosos, modelos de dados mais ricos, integrando uma componente semântica que facilita a interoperabilidade das soluções de gestão. Torna também mais fácil o desenvolvimento de soluções de gestão para cenários heterogéneos, com diferentes fabricantes, diferentes arquitecturas computacionais e diferentes sistemas operativos. Fica a dúvida se a interoperabilidade acrescida conseguirá vencer os

motivos de ordem comercial e se fará com que os fabricantes desenvolvam suporte de gestão para equipamentos desenvolvidos por outros fabricantes.

O aumento da complexidade das soluções de gestão tem um preço em termos de requisitos computacionais: a crescente quantidade de informação de gestão requer maiores quantidades de memória dos elementos de gestão; requer maiores tempos de resposta das entidades devido ao maior custo de codificação e descodificação da informação; e requer ainda maior largura de banda dos sistemas de comunicação entre elementos de gestão. É por isso necessário avaliar o impacto das diversas tecnologias na capacidade de desempenho das soluções de gestão, em particular a sua escalabilidade de forma a não comprometer a possibilidade de desenvolver sistemas de gestão integrados em cenários de gestão de dimensão superior.

A Figura 2.38 ilustra a distribuição temporal do aparecimento das diversas tecnologias durante as últimas duas décadas. A diversidade observada ajuda a explicar o facto de as diversas tecnologias de gestão desenvolvidas pelo IETF não se terem implantado no seio da indústria e que, apesar de lhe terem sido apontados vários defeitos, a tecnologia SNMP, ainda é a norma de gestão de redes mais difundida.

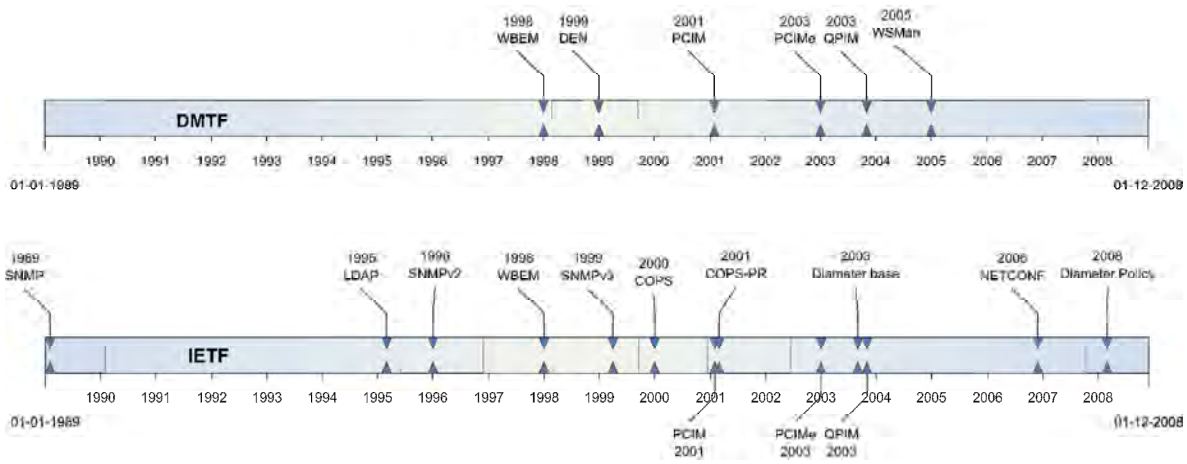

Figura 2.38 – Cronograma do desenvolvimento das tecnologias de gestão.

3 Redes e Serviços de Próxima Geração

As últimas duas décadas trouxeram enormes desenvolvimentos nas comunicações móveis cujos reflexos podem ser observados, tanto na evolução das tecnologias de rede, como na vulgarização da utilização dos serviços que essas tecnologias permitiram.

Desde o aparecimento da primeira geração de redes celulares (1G) até ao presente ocorreu uma enorme evolução. O desenvolvimento das redes 1G (1ª Geração) começou nos anos 80 e baseou-se no conceito de uma rede analógica de comunicações sem fios, cujo único serviço disponibilizado era o serviço de voz.

No início dos anos 90 iniciou-se o desenvolvimento da segunda geração de redes de comunicações móveis (2G – 2ª Geração) que se distinguia da geração anterior pelo facto de ser completamente digital. Apesar de ser digital, era uma rede de comutação de circuitos sendo os únicos serviços disponibilizados o serviço de voz e o serviço de mensagens (*Short Message Service* - SMS). Na Europa a versão de rede 2G desenvolvida foi o *Global System for Mobile Communications* (GSM), que nos anos 90 teve uma enorme vulgarização. Durante a segunda metade da década de 90 foram adicionados à segunda geração serviços de dados e de troca de pacotes. Essa extensão de serviços foi designada de 2,5G e trouxe os serviços da Internet para o mundo das comunicações móveis.

Os standards para os sistemas da terceira geração (3G – 3ª Geração) foram definidos em 1999: na Europa foi definido o *Universal Mobile Telecommunications System* (UMTS); nos Estados Unidos foi definido um standard derivado da tecnologia CDMA2000; e no Japão a NTT DoCoMo desenvolveu uma rede baseada em W-CDMA. As redes de 3G caracterizam-se por: manterem suporte de mobilidade, apesar de possuírem raios de cobertura menores; disponibilizarem taxas de transferência de informação muito mais elevadas do que as redes anteriores; suportarem vários serviços de comunicação multimédia; possuírem redes de core baseadas em IP, apesar de não fornecerem garantias de Qualidade de Serviço (QdS).

A Tabela 3.1 sumaria a evolução tecnológica das redes nas três primeiras gerações, relativamente a diversas características estudadas.

Para além da evolução das comunicações celulares várias tecnologias de comunicação sem fios têm sido desenvolvidas, algumas das quais com uma disseminação alargada. Na área das redes pessoais (*Personal Area Networks* - PAN) criou-se o *Bluetooth* [61], que apesar de ter nascido como uma tecnologia proprietária, foi normalizada pelo IEEE (norma 802.15). Tal como os

sistemas baseados em comunicações por infravermelhos, permite a constituição de redes sem fios de pequeno débito e aplicável em pequenas distâncias.

Tabela 3.1 - Características das várias gerações de comunicações móveis.

CARACTERÍSTICA	1G	2G	2.5G	3G
Comercialização	1985	1992	1995	2002
Frequência radio	400-800 MHz	800-900 MHz, 1800-1900 MHz		2GHz
Largura de banda	2,4 – 30 Kbps	9,6 – 14,4 Kbps	171 – 384 Kbps	2-5 Mbps
Tecnologia de acesso	FDMA	TDMA, CDMA		CDMA
Cobertura celular	Larga	Média		Pequena
Rede de core	Rede de operadores	Rede de operadores		Rede de operadores, redes IP
Suporte de mobilidade	Sim	Sim	Sim	Sim
Roaming	Nacional	Internacional		Internacional
Serviços	Voz	Voz, SMS	Voz, SMS, Dados	Voz, Dados, Multimédia

O IETF desenvolveu também uma tecnologia para redes locais sem fios (*Wireless Local Area Network* - WLAN), baseada no protocolo IEEE 802.11 [62], que opera em frequências à volta de 2,4 GHz, com taxas de transferência desde 11 Mbps no modo 802.11b, até aos 54 Mbps, nos modos 802.11a e 802.11g. O WiFI, designação como também é conhecida a tecnologia 802.11 do IEEE, tornou-se num dos mais populares meios de acesso à Internet.

A tecnologia (*Worldwide Interoperability for Microwave Access – WiMAX*) ou IEEE 802.16 [63], tem vindo a ser desenvolvida pelo IEEE como uma alternativa de acesso de banda larga especialmente concebida para zonas rurais, onde o custo de instalação de infra-estruturas de rede tradicionais torna difícil a rentabilização dos investimentos, devido à baixa densidade populacional.

3.1 Arquitecturas de rede NGN

Os operadores de acesso têm assistido nos últimos anos a uma baixa progressiva nos lucros de exploração das suas redes, apesar de as taxas de utilização continuarem a crescer. A política de definição de tarifas planas para o acesso, onde os utilizadores podem gerar uma quantidade livre de tráfego, ajudou à massificação do acesso à Internet. Contudo, o efeito ao nível das receitas não foi de crescimento proporcional.

Não tem sido prioridade dos operadores o investimento na implementação de mecanismos de QdS que lhes poderiam criar uma diferenciação no tratamento do tráfego, bem como uma correspondente diferenciação na tarifação do mesmo. Na falta desse tipo de mecanismo todos os pacotes recebem o mesmo tratamento, o melhor esforço, sendo a adição de novos recursos a única

solução que o operador tem para descongestionar a infra-estrutura da rede. Novos *links* e novos *routers*, representam investimentos financeiros que os operadores de transporte de dados não têm sabido capitalizar.

Também durante estes últimos anos novos serviços têm surgido, tais como, o envio de vídeo, as redes *Peer-to-Peer* (P2P) para partilha de dados e os serviços de voz transportada em IP (VOIP). No caso das redes P2P são geradas quantidades enormes de tráfego em consequência da cópia massiva de ficheiros entre clientes dessas redes. A crescente utilização de serviços de vídeo, de que o *Youtube* é o exemplo mais representativo, gera enormes quantidades de tráfego, que também sobrecarrega as redes dos operadores de transporte. Os serviços de VOIP têm ainda efeitos mais perversos: além da geração de quantidades enormes de tráfego que serviços como o *Skipe* criam, roubam clientes aos operadores de voz tradicionais que tipicamente também pertencem às empresas dos operadores de dados.

Apesar do aumento de tráfego nas redes de dados não ter criado grandes aumentos de receitas, outras empresas prestadoras de serviços como o *Youtube*, o *Skipe*, têm crescido imenso e gerado enormes receitas através da venda de serviços e / ou das receitas de publicidade.

Perante este cenário os operadores têm-se associado em torno de várias iniciativas como: *Third Generation Partnership Project* (3GPP) [64], *Telecommunications and Internet converged Services and Protocols for Advanced Networking* (TISPAN) [65], o *TeleManagement Forum* (TMForum) [66], *Open Mobile Alliance* (OMA) [67], IPSphere [68], entre outras, com vista à normalização e desenvolvimento de uma solução para a perda de valor acrescentado que os serviços que prestam têm sofrido. A Figura 3.1 ilustra as contribuições mútuas entre as diversas entidades envolvidas no processo de normalização de NGN [69].

A normalização das redes NGN iniciou-se em 2004 com a publicação da recomendação Y.2001 do ITU-T designada de "*General overview of NGN*", à qual se seguiu a recomendação Y.2011 [70] onde se definia um modelo de referência para as redes da próxima geração. Estas normas influenciaram os trabalhos de definição da arquitectura das redes NGN levada a cabo por outras organizações, entre as quais o 3GPP que na altura procurava definir a arquitectura de uma rede capaz de disponibilizar conteúdos multimédia a utilizadores móveis. No âmbito dos esforços de desenvolvimento desta arquitectura foi proposta uma arquitectura de rede modular designada de *IP Multimedia Subsystem* (IMS) [71] que se descreve em 3.1.2. e que curiosamente viria a ser incorporada na generalidade das propostas de arquitectura das redes NGN.

Uma rede de próxima geração é uma rede de comutação de pacotes baseada no protocolo IPv6, capaz de fornecer serviços de rede tão distintos como acesso à Internet ou serviços de telecomunicações através de meios de acesso de banda larga com diversas tecnologias de acesso.

As subsecções seguintes descrevem as principais iniciativas de normalização de redes NGN.

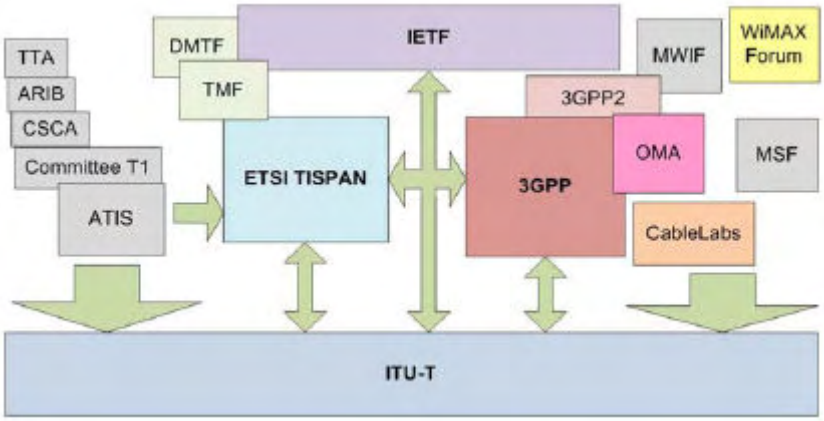

Figura 3.1 - Contribuições entre entidades de normalização das redes NGN [69].

3.1.1 ITU-T

Na recomendação Y.2012 do ITU-T é proposta uma arquitectura de rede ilustrada na Figura 3.2, bem como são identificado os seguintes requisitos [72]. É proposto um transporte de informação baseado no protocolo IPv6 com suporte de QdS entre extremos e suporte generalizado de mobilidade. É prevista uma separação das funções de controlo como controlo de barreiras rádio, controlo de sessões, controlo de aplicações e serviços, bem como o fornecimento de interfaces abertos. Deverá ser suportada uma grande diversidade de serviços, de aplicações e de mecanismos que deverão ser facilmente integrados graças a interfaces de integração de serviços normalizados. O fornecimento de acesso a utilizadores de diferentes operadores de serviço deverá ser suportado e as funcionalidades do nível dos serviços deverão ser independentes das tecnologias de transporte. É recomendado que a interligação das redes NGN com redes legadas seja implementada através da disponibilização de interfaces abertos, bem como que seja realizada a convergência de serviços entre as redes móvel e fixa.

Um dos aspectos mais importantes da arquitectura proposta é a independência entre a gestão dos serviços fornecidos e a gestão da rede de transporte, sendo a arquitectura composta por dois estratos: o estrato do transporte e o estrato do serviço. O estrato de serviço é responsável pela sinalização das aplicações, ao passo que o estrato de transporte é responsável pela entrega fiável dos pacotes de dados e do controlo de fluxo.

A função de controlo de transporte pertence ao estrato de transporte mas está interligada com o estrato de serviço, servindo como intermediário entre ambos os estratos. Efectua o controlo

de admissão com base nas políticas da rede e na disponibilidade dos recursos, bem como efectua a reserva de recursos de rede de forma a servir os pedidos previamente aceites.

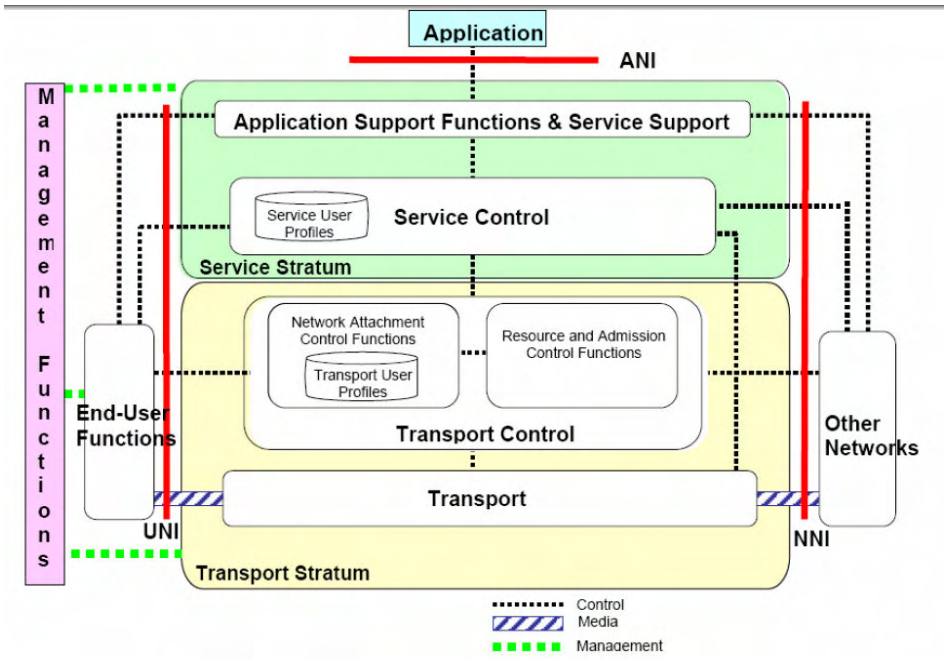

Figura 3.2 - Arquitectura NGN do ITU [72].

A rede implementa mecanismos de prioritização do tráfego e de controlo de admissão e fornece ao tráfego garantias de QdS entre extremos envolvidos na comunicação. Permite acesso aos diversos serviços oferecidos independentemente da tecnologia da rede de acesso utilizada, sendo por isso dita como agnóstica em termos de tecnologia de acesso.

A rede NGN do ITU-T suporta mobilidade de utilizadores entre diferentes redes de acesso, bem como a mobilidade dos utilizadores entre diferentes tecnologias de acesso à rede, permitindo um acesso ubíquo dos utilizadores aos diferentes serviços disponibilizados. Efectua ainda uma adaptação das condições de acesso de acordo com as preferências previamente definidas por cada utilizador.

O elemento principal de controlo de transporte é o *Resource and Admission Control Functions* (RACF), que se encontra ilustrado na Figura 3.3. É constituído por duas componentes: a *Policy Decision Functional Entity* (PD-FE) e a *Transport Resource Control Functional Entity* (TFC-FE).

A PD-FE recebe pedidos da camada de controlo de serviços e transforma-os em classes de serviço independentes da tecnologia de transporte, definindo parâmetros como a largura de banda, o atraso, a variância do atraso ou a percentagem de perda de pacotes. Interroga também a TRC-FE para saber sobre a disponibilidade dos recursos de rede para atender aos pedidos recebidos. Para ter em conta as capacidades da rede de transporte e a informação constante no perfil dos utilizadores

(*e.g.*:, registo de acesso, autenticação, serviços autorizados, etc.) o *Policy Decision Physical Entity* (PD-PE) comunica com o *Network Attachment Control Functions* (NACF).

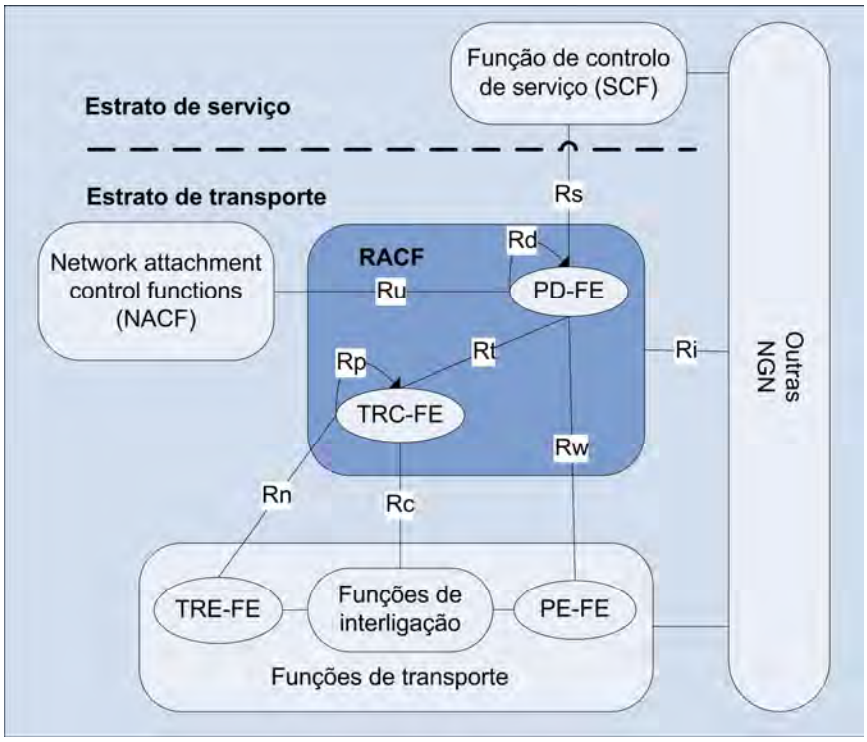

Figura 3.3 - Arquitectura do RACF [73].

A TFC-FE efectua controlo de admissão e gere os recursos relativos aos segmentos de rede de que é responsável. Configura também a *Transport Resource Enforcement Resource Entity* (TRE-FE), para que esta implemente as decisões relativas ao controlo de admissão e à configuração de recursos que tomou. Para além disso o TRC-FE também monitoriza a topologia da rede, bem como o estado dos recursos da rede de que é responsável.

O PD-FE controla o dispositivo de transporte designado de *Policy Enforcement Functional Entity* (PE-FE) que se localiza na fronteira da rede, implementado sob a forma de uma *gateway*, ou de um *router* de fronteira. O PD-FE controla a QdS da rede controlando o PE-FE do extremo da rede.

Os protocolos de comunicação das interfaces identificadas na Figura 3.3 com as designações de *Rs*, *Rp*, *Rw*, *Rc*, e *Rt* foram definidos e encontram-se identificados na Tabela 3.2. Os restantes não foram ainda definidos.

Tabela 3.2 - Identificação dos protocolos de comunicação na NGN ITU-T.

INTERFACE	PROTOCOLO
Rs	Diameter
Rp	Resource Connection Initiation Protocol (RCIP)
Rw	COPS-PR H.248 Diameter
Rc	COPS-PR SNMP
Rt	Diameter

O controlo de QdS é proposto através de dois métodos: o de aprovisionamento e o de *outsourcing*. No modelo de aprovisionamento (Figura 3.4) o PD-FE envia a política de QdS para o equipamento de transporte (PE-FE), assim que o pedido de QdS é recebido do *Service Control Function* (SCF). No modelo de *outsourcing* (Figura 3.5) o PD-DE recebe o pedido de QdS do PE-FE, depois do PE-FE ter recebido o pedido do QdS do seu congénere da rede com quem está em comunicação.

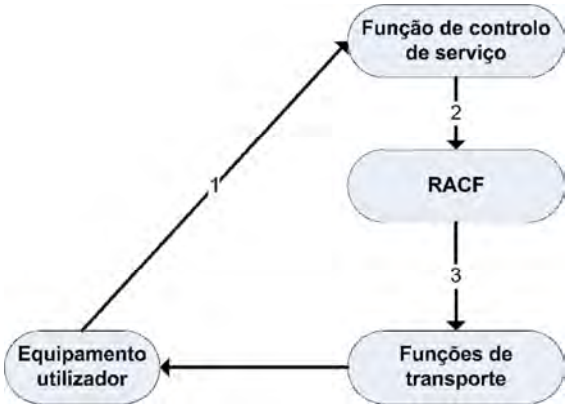

Figura 3.4 - Modelo de aprovisionamento.

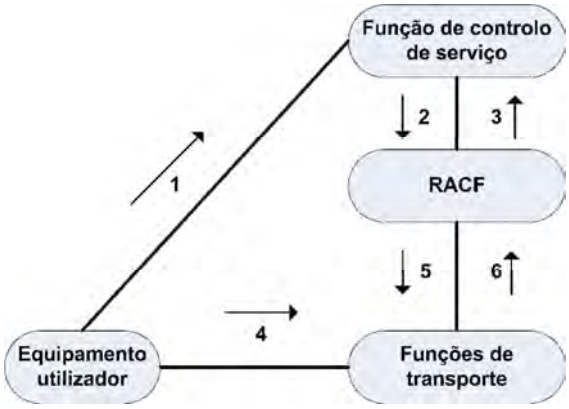

Figura 3.5 - Modelo de *outsourcing*.

3.1.2 3GPP-IP Multimedia Subsystem (IMS)

IP Multimedia Subsystem (IMS) representa uma arquitectura de uma plataforma NGN para fornecimento de serviços multimédia a utilizadores móveis. O seu desenvolvimento ocorreu dentro do consórcio 3GPP tendo sido posteriormente adoptado e apoiado por iniciativas como TISPAN, *Broadband Forum* e OMA.

A filosofia de base na proposta, ilustrada na Figura 3.6, mostra uma rede com um elemento central chamado de IMS. Este recebe os pedidos de serviço por parte do utilizador encaminha-os para os servidores correspondentes, processando e gerindo as redes de transporte da informação.

Figura 3.6 - Filosofia do IMS.

Fornece também aos operadores de serviços uma abstracção da rede que lhes permite efectuar o desenvolvimento dos serviços sem ter em conta os pormenores de funcionamento e gestão da própria infra-estrutura de comunicações. Permite-lhes assim um desenvolvimento dos serviços de uma forma mais fácil e rápida, melhorando o tempo de implementação de novos serviços. Simultaneamente permite o controlo de todos os acessos aos serviços, uma vez que é a plataforma de IMS que medeia todos os pedidos de serviço só permitindo o acesso a fornecedores de serviços registados.

A rede IMS é uma rede *Session Initiation Protocol* (SIP) onde o terminal requer acesso a serviços utilizando o protocolo de estabelecimento de sessões SIP [51]. Na comunicação entre as entidades da arquitectura, são utilizados protocolos desenvolvidos dentro do IETF, tendo havido uma preocupação clara por utilizar protocolos simples e de fácil implementação. A atitude do consórcio tem sido de cooperação aberta com outras organizações: o IETF por exemplo, onde foram desenvolvidos os protocolos de comunicação utilizados; a OMA [67], onde tem vindo a ser proposta a plataforma de desenvolvimento de serviços; e o TISPAN [65], onde têm sido definidas muitas das especificações de entidades da rede IMS.

A arquitectura IMS do 3GPP, representada na Figura 3.7, é uma arquitectura modular com várias camadas, onde se desagrega a gestão dos equipamentos de rede do desenvolvimento dos serviços e dos pormenores de implementação das várias tecnologias de acesso à rede. A gestão dos equipamentos realiza-se a nível do IMS, que opera a nível das camadas de transporte e controlo, que através de um conjunto de *gateways* apropriadas a cada rede de acesso controlam os fluxos de dados provindos ou destinados a cada uma das diferentes redes de acesso. Disponibiliza também uma plataforma de serviços aberta aos provedores de serviços para que estes possam desenvolver aplicações que interajam com a plataforma de gestão.

As funcionalidades de cada uma das camadas são implementadas por um conjunto de entidades funcionais que se encontram ilustradas na Figura 3.7.

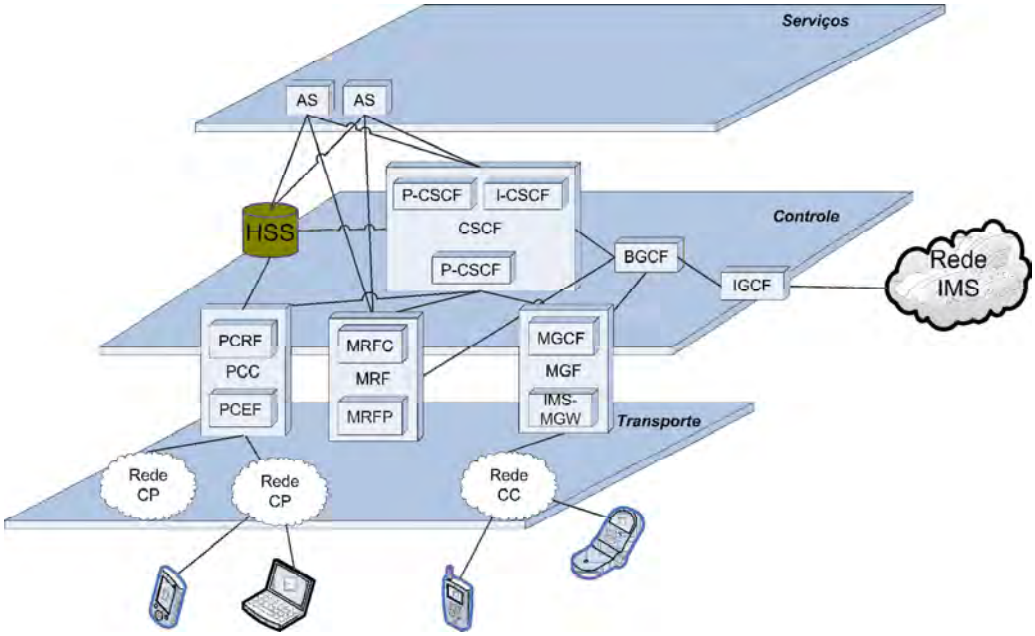

Figura 3.7 - Arquitectura de referência do IMS.

Na camada de controlo podem-se encontrar as entidades envolvidas nas decisões de estabelecimento de novos serviços como *Call Session Control Function* (CSCF), na gestão da informação relativa aos utilizadores *Home Subscriber Server* (HSS), com o controlo das dos fluxos de dados como o *Policy and Charging Control Function* (PCRF) e o *Multimedia Resource Function* (MRF), e entidades que interligam vários domínios IMS.

O HSS (Figura 3.8) é um repositório que mantém a informação relacionada com as subscrições do utilizador, sendo utilizado pelas entidades de rede que gerem chamadas e sessões. Cada rede de um operador pode possuir um ou vários HSS, dependendo do número de subscritores e da capacidade do equipamento.

Figura 3.8 - HSS e as entidades com quem estabelece comunicação.

O HSS mantém a seguinte informação relacionada com o utilizador: número e endereço; informação de segurança: informação de controlo de acesso para autorização e autenticação; e informação acerca do perfil do utilizador.

A Figura 3.8 representa os sub-módulos do HSS, bem como a comunicação entre o HSS e as outras entidades da rede. Na rede de comutação de pacotes o HSS actua como um *Home Location Register* (HLR) ou um *Authentication Center* (AuC). Na rede IMS o HSS fornece suporte às suas entidades de controlo, como CSCF. Na rede de comutação de chamadas o HSS fornece funcionalidades de HLR e AuC.

A Figura 3.9 ilustra o conjunto de funções lógicas fornecido pelo HSS, bem como as ligações que este tem com cada tipo de rede:

- Suporta a mobilidade do utilizador através dos sub-domínios de comutação de chamadas, de pacotes e sub-domínio IMS;
- Fornece suporte às entidades de controlo de sessão nos três domínios e efectua a geração de *tokens* para suporte de segurança do utilizador;
- Gere a informação de identificação do utilizador e faz a autorização dos serviços para o utilizador e actualiza a informação relevante acerca dos serviços disponibilizados ao utilizador em cada uma das entidades da rede.

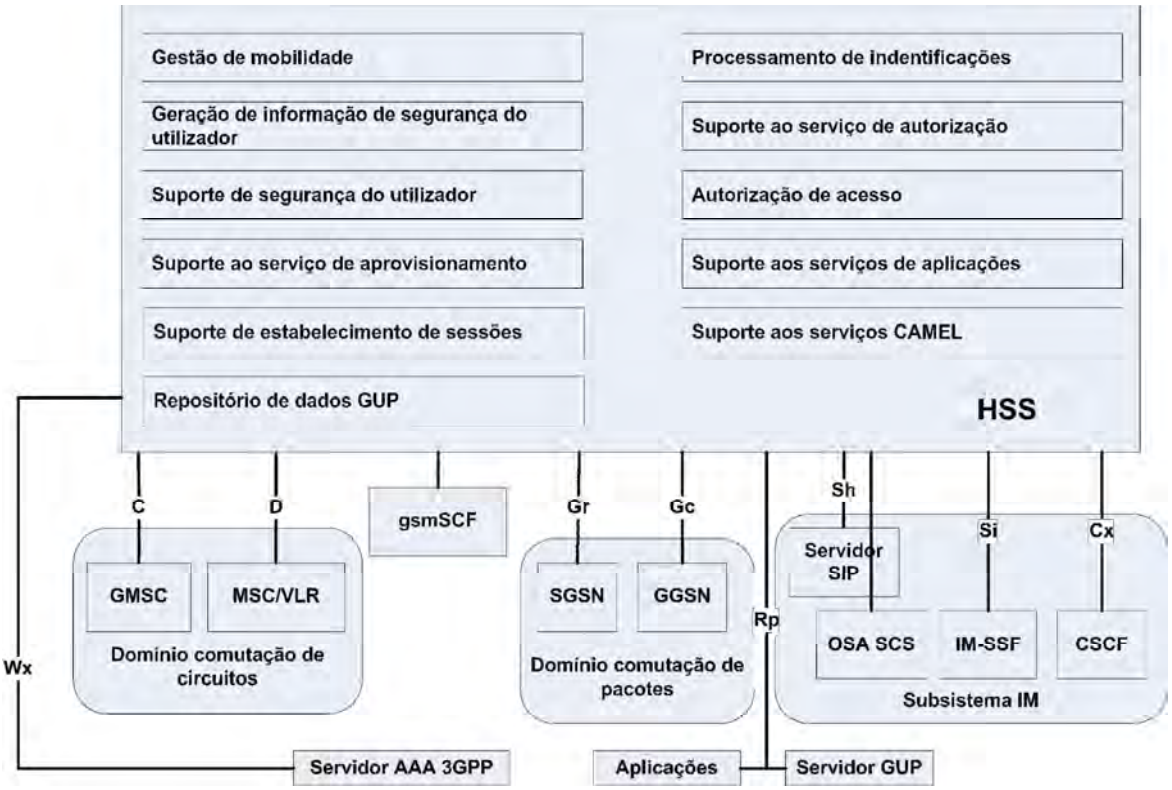

Figura 3.9 - HSS e as entidades com que comunica [74].

O CSCF é o elemento central de uma rede de IMS (Figura 3.10). Ele estabelece, monitoriza, suporta e liberta sessões multimédia e gere as interacções com os serviços do utilizador. O CSCF contêm três componentes: *Proxy* – CSCF (P-CSCF); o *Interrogating* – CSCF (I-CSCF); e o *Serving* – CSCF (S-CSCF) [75].

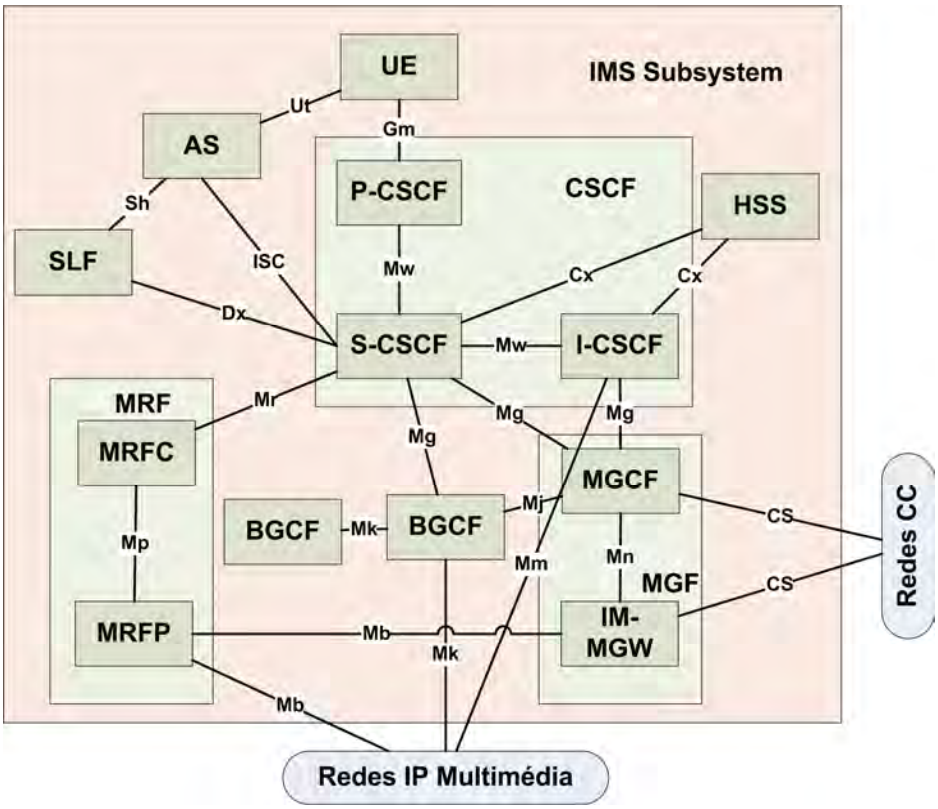

Figura 3.10 - Detalhe da arquitectura de referência do IMS [74].

A *Breakout Gateway Control Function* (BGCF) determina o próximo nó para o encaminhamento de uma mensagem SIP. O reencaminhamento pode ser feito com base no protocolo recebido, em informação administrativa ou na base de dados de acesso, sendo o reencaminhamento feito com base nas seguintes regras:

- No caso de o destino da comunicação se encontrar dentro da rede de outro IMS o BGCF encaminha essa informação para o I-CSCF da rede desse IMS.
- Se a BGCF determinar que o destino da comunicação se encontrar dentro de uma rede pública de comutação de circuitos, e se a interligação com a rede destino se der dentro da sua rede, ela escolhe uma MGCF que encaminhe a mensagem para essa rede de comutação de circuitos.
- Se a BGCF determinar que a mensagem se destina a uma rede PTSN de outro IMS reencaminhará a mensagem para outro BGCF.

A BGCF é definida pela TS 132.002 e podem existir várias instâncias dessa entidade dentro de um domínio IMS.

O *Interconnection Border Control Function* (IBCF) fornece funcionalidades ao nível da camada SIP / SDP, permitindo a interligação entre domínios de dois operadores. Permite também: a comunicação entre aplicações SIP IPv4 e IPv6; esconder a topologia de rede; fornecer funções ao nível do plano de controlo; a verificação da sinalização SIP; a selecção do ponto de ligação mais apropriado; e a geração de registos de utilização.

O *Multimedia Resource Function* (MRF) gere recursos da rede de *core* de forma a implementar serviços de conferência. Recebe pedidos do *Application Function* (AF) via CSCF de marcação de conferências e com base na informação desses pedidos, como hora, data e lista de participantes, efectua a gestão dos recursos necessários à implementação desses pedidos.

O *Multimedia Gateway Function* (MGF) fornece interligação da rede IMS com as redes de comutação de chamadas. Faz a adaptação de conteúdos com recurso a *codec's* e controla a *gateway* de interligação.

Apesar de se considerar não pertencerem ao IMS, os servidores de aplicações (*Application Server* - AS) fornecem serviços de multimédia de valor acrescentado à plataforma de IMS (Figura 3.11). Os AS são entidades funcionais externas que são colocadas no topo da arquitectura do IMS. Podem residir na rede origem do utilizador, ou então na rede de um operador externo confiável. As principais funcionalidades implementadas por um AS são: o processamento e resposta à sinalização SIP recebida do IMS; o alojamento e execução de serviços; a geração de pedidos SIP; e o envio de informação de registo de utilização para entidades de contabilização designadas de *Offline Charging System* (OFCS) e *Online Charging System* (OCS) respectivamente. Contudo, os serviços oferecidos pelos AF não se limitam a serviços SIP, uma vez que os operadores podem oferecer outros de serviços, tais como serviços baseados na plataforma de desenvolvimento de serviços *Open Service Architecture Service Capability Server* (OSA SCS) ou CAMEL IMS *Service Switching Function* (IM-SSF).

As API de serviços baseadas em OSA permitem que os operadores utilizem funcionalidades do IMS como: controlo de chamadas, interacção com o utilizador, visualização do estado das chamadas, visualização do estado do utilizador, controlo da sessão de dados, consulta de características do utilizador e gestão de registos de utilização e contabilização. Fornece ainda segurança nas ligações à rede IMS normalmente não implementadas pelos CSCF, uma vez que as APIs OSA por defeito implementam funcionalidades de autenticação, autorização e de descoberta. A IM-SSF foi introduzida na arquitectura IMS para possibilitar o suporte a serviços legados que foram desenvolvidos para o ambiente de serviços CAMEL.

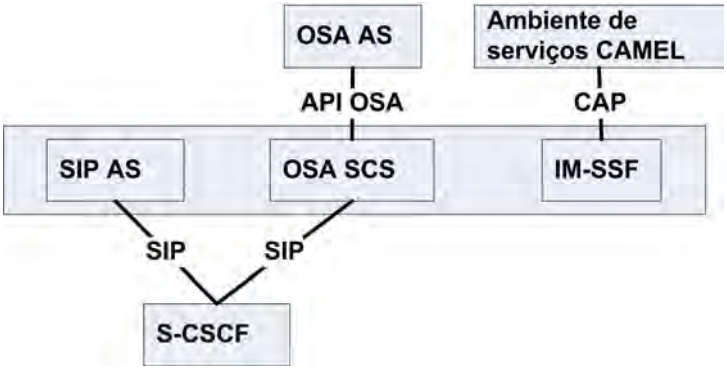

Figura 3.11 - Vários tipos de servidores de aplicações para a plataforma IMS.

O terminal do utilizador (*User Equipment* - UE), apesar de não pertencer à arquitectura do IMS é uma entidade que comunica com o IMS. O terminal está ligado à rede de acesso mas envia os pedidos SIP à plataforma de CSCF que o serve. A aprendizagem do endereço do CSCF é feita no processo de registo do terminal na rede de acesso, através da informação enviada pelos servidores de DHCP e de DNS segundo um procedimento descrito em [75]. O CSCF reencaminha os pedidos ao AF e devolve a resposta dada ao terminal.

A Tabela 3.3 enumera o conjunto de entidades existentes numa rede IMS bem como as suas funcionalidades e o documento onde são especificadas.

Tabela 3.3 - Lista das entidades funcionais da rede IMS.

ENTIDADE	FUNCIONALIDADE	ESPECIFICAÇÃO
Call Session Control Function(CSCF)	Controlo das sessões SIP, encaminhamento para servidor correcto	ETSI TS 123 517
Media Gateway Function (MGF)		ETSI TS 123 517
Multimédia Resource Function (MRF)		ETSI TS 123 517
Breakout Gateway Control Function(BGCF)		ETSI TS 123 517
Interconnection Border Control Function(IBCF)	Implementa a interface entre domínios IMS diferentes	ETSI TS 182 006
Policy and Charging Function (PCC)		ETSI TS 123 203
AF		
Terminal utilizador (UE)		

Como ilustrado na Figura 3.10, as interfaces entre todas as entidades estão já identificadas. A Tabela 3.4 lista os pontos de referência da plataforma IMS e identifica, para cada um deles, as entidades que interliga, o protocolo de comunicação utilizado na comunicação e o documento normativo.

Tabela 3.4 - Lista de pontos de referência dentro do core IMS.

NOME	ELEMENTOS	PROTOCOLO	ESPECIFICAÇÃO
Mg	MGCF, CSCF	SIP	ETSI TS 123 002
Mr	CSCF, MRFC	SIP	ETSI TS 123 002
Mw	CSCF, CSCF	SIP	ETSI TS 123 002
Mi	CSCF, BGCF	SIP	ETSI TS 123 006
Mj	BGCF, MGCF	SIP	ETSI TS 123 002
Mk	BGCF, BGCF	SIP	ETSI TS 182 006
Mx	CSCF ou BGCF, IBCF	SIP	ETSI TS 182 006

O P-CSCF é o primeiro ponto de contacto entre o UE e o sistema IMS. O seu endereço é descoberto pelo terminal do utilizador segundo um processo previamente conhecido que é definido em [75]. O P-CSCF comporta-se como uma *proxy* descrita na RFC 3261, na medida em que aceita pedidos que serve ou que reencaminha para outras entidades. Entre as suas funcionalidades encontram-se:

- Encaminhamento dos pedidos de registo SIP do UE para o ponto de entrada de outro domínio, utilizando para isso o domínio de origem do cliente;
- Encaminhamento de mensagens de estabelecimento de sessões SIP, entre UE e o servidor SIP;
- Compressão e descompressão de mensagens SIP;
- Verificação da informação da rede de acesso nos pedidos enviados pelo terminal ao servidor SIP;
- Tratamento da autorização dos processos de controlo de acesso aos recursos da rede como definido no TS 23.203;
- Manutenção de associações de segurança entre si e o terminal como definido no TS 33.203.

O I-CSCF é o ponto de contacto da rede de um operador para todas as ligações externas de entrada. Podem existir vários I-CSCF na rede de um operador, tendo as seguintes funções: atribuição de um S-CSCF a um utilizador na altura do seu registo na rede; encaminhamento de pedidos SIP vindos de outras redes para o S-CSCF; obtenção do endereço do S-CSCF de cada HSS; e reencaminhamento das mensagens SIP com base na informação obtida do HSS [75].

O I-CSCF pode ainda fazer reencaminhamento de mensagens SIP, no caso de verificar através da informação obtida pelo HSS que o servidor SIP não se encontra na rede do seu operador.

O S-CSCF efectua controlo de sessão de serviços SIP do terminal, mantendo o estado das sessões necessário ao suporte dos serviços. Podem existir na rede de um operador vários S-CSCF, que entre outras coisas efectuam [75]:

- Aceitação dos pedidos de registo e disponibilização dessa informação através de um servidor de localização, tal como descrito na RFC 3261;

- Controlam e identificam univocamente as sessões activas, barrando sessões não autorizadas;
- Notificam os subscritores das sessões sobre as alterações por estas sofridas;
- Actua como um *proxy* do servidor, encaminhando pedidos que recebe do terminal para o servidor de aplicações, podendo no entanto servir alguns;
- Interage com a plataforma dos serviços em nome do utilizador de forma a garantir o suporte dos serviços;
- Encaminha os pedidos para o BGCF no caso de chamadas destinadas a outra rede de comutação de pacotes;
- Verifica as características do pedido SIP, mediante as características dos serviços do operador e se o destinatário da chamada subscreveu o serviço;
- Altera o encaminhamento das mensagens SIP, no caso de a chamada se destinar à rede de comutação de circuitos e entrega-a ao BGCF.

Para o suporte de sessões de emergência é proposta na versão 8.0.0 da arquitectura funcional [74] uma entidade designada de *Emergency CSCF* (E-CSCF).

A Tabela 3.5 resume as características das várias entidades que compõem a arquitectura do CSCF.

Tabela 3.5 - Lista de entidades funcionais da arquitectura do CSCF.

ENTIDADE	FUNCIONALIDADE	ESPECIFICAÇÃO
P-CSCF	*Proxy* do CSCF que media a comunicação entre o terminal e S-CSCF encarregue de os entender.	TS 182 006
I-CSCF	Recebe as comunicações SIP oriundas de fora do domínio do operador que se destinam a um S-CSCF nessa rede.	TS 182 006
S-CSCF	Controla acesso das sessões SIP, encaminha pedidos entre P-CSCF e servidores de aplicações.	TS 182 006
E-CSCF	Entidade encarregue de gerir comunicações de emergência.	TS 192 009

Na versão 7 da arquitectura do IMS foi efectuada a aglomeração das entidades de políticas (*Service Based Local Policy*) e de registo de utilização (*Flow Based Charging*) existentes nas versões anteriores. Foi proposta uma plataforma conjunta designada de *Policy Control and Charging* (PCC) [76]. A arquitectura desta plataforma, ilustrada na Figura 3.12, é constituída pelas seguintes entidades: o *Policy and Charging Enforcement Function* (PCEF), o *Policy and Charging Rules Function* (PCRF), o *Application Function* (AF), o *Online Charging System* (OCS), o *Offline Charging System* (OFCS), e o *Subscription Profile Repository* (SPR).

A arquitectura da plataforma PCC é o resultado da distribuição da plataforma de controlo de recursos baseada em políticas existente nas versões 5 e 6 do IMS, onde existia uma entidade

designada de *Policy Definition Function* (PDF). A proposta actual prevê uma divisão do elemento PDF num elemento decisor (PCRF) e num elemento executor de políticas (PCEF) que deverá ser colocado junto à *gateway* de forma a colocar em prática as decisões tomadas pelo PCRF. A comunicação entre ambos é efectuada através da interface *Gx* [77], que é implementada utilizando o protocolo Diameter.

O PCRF é o elemento que toma decisões de controlo de admissão com base no perfil dos utilizadores, na disponibilidade dos recursos e nas regras de atribuição de recursos previamente recebidas. Efectua também operações de gestão de recursos enviando para isso instruções através de PCEF. A sua funcionalidade é em tudo semelhante a um *Bandwidth Broker* [78].

A consulta ao perfil do utilizador é feita com base no acesso à informação do SPR através da interface *Sp*. O PCEF além de implementar as decisões de controlo de admissão e de configuração de recursos definidas pelo PCEF, efectua também a recolha de informação sobre a utilização dos recursos que envia às entidades responsáveis por fazer o registo de utilização. Essas entidades, o OFCS e o OCS, comunicam com o PCEF através das interfaces *Gz* e *Gy*, respectivamente.

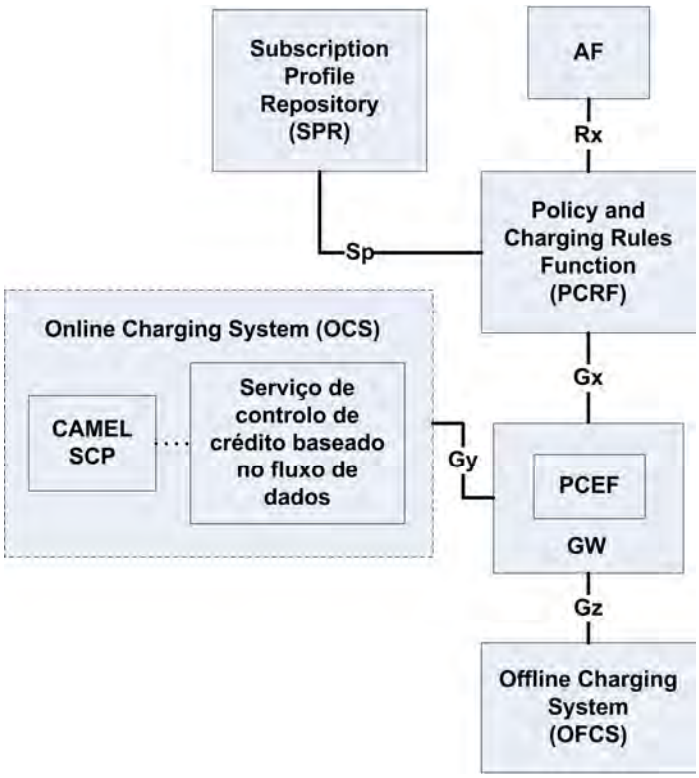

Figura 3.12 - Arquitectura da plataforma PCC [52].

A AF é uma entidade funcional que requisita recursos de rede ao PCRF. Pode ser, por exemplo um CSCF, que ao tomar a decisão de aceitar uma nova sessão SIP, contacta o PCRF com

o objectivo de saber se os recursos da rede estão disponíveis para servir essa sessão. A comunicação entre o AF e o PCRF é feita através da interface *Rx* [79] e é implementada utilizando o protocolo Diameter. A Tabela 3.6 apresenta a lista de entidades pertencentes à arquitectura do PCC, a sua funcionalidade e o documento que efectua a sua especificação.

Tabela 3.6 - Lista de entidades funcionais da arquitectura do PCC.

ENTIDADE	FUNCIONALIDADE	ESPECIFICAÇÃO
AF	Entidade requerente de recursos da rede	
SPR	Repositório com o perfil do utilizador	
PCRF	PDP da arquitectura	ETSI TS 123 203
PCEF	PEP da arquitectura	ETSI TS 123 203
OCS	Sistema de contabilização *online*	ETSI TS 132 240
OFCS	Sistema de contabilização da utilização de recursos *offline*	ETSI TS 132 240

A Tabela 3.7 sumaria o conjunto de interfaces que interligam as entidades da arquitectura do PCC, o protocolo utilizado na sua comunicação, bem como o documento que as especifica. Tal como o protocolo SIP, o protocolo Diameter tem uma forte utilização nas interfaces de comunicação da plataforma IMS.

Tabela 3.7 - Lista de interfaces dos elementos da arquitectura PCC.

NOME	ELEMENTOS	PROTOCOLO	ESPECIFICAÇÃO
Rx	AF, PCRF	Diameter	3GPP TS 29.214
Sp	SPR, PCRF	Diameter	3GPP TS 23.203
Gx	PCRF, PCEF	Diameter	3GPP TS 29.212
Gz	PCEF, OFCS	Diameter	3GPP TS 32.240
Gy	PCEF, OCS	Diameter	3GPP TS 32.290

O *Media Gateway Function* é composto por duas entidades: a *Media Gateway Control Function* (MGCF) e a *IP Multimedia Subsystem Media Gateway Function* (IMS-MGW).

O MGCF efectua a configuração da IMS-MGW, através de uma interface normalizada, alocando e libertando recursos da IMS-MGW, bem como alterando a utilização que é feita por esses recursos. Comunica com o CSCF, o BGCF e com as redes de comutação de circuitos, fazendo também conversão de protocolos de sinalização dessas redes e SIP. MGCF é especificada na TS 123 002 e determina qual o próximo nó IP, com base na informação de sinalização recebida quando a plataforma de IMS receber chamadas das redes legadas.

A IMS-MGW interliga redes de comutação de chamadas com redes de comutação de pacotes. Pode suportar controlo de acesso e processamento de conteúdos como: transcodificação, cancelamento de eco, ou *conference bridging*. A IMS-MGW interliga por exemplo as redes UMTS e GSM; e necessita de recursos para transpor a informação das chamadas dessas redes para a rede IMS. A Tabela 3.8 resume as principais características dos elementos que compõem a arquitectura do MGF.

Tabela 3.8 - Lista de entidades funcionais da arquitectura MGF.

ENTIDADE	FUNCIONALIDADE	ESPECIFICAÇÃO
Multimedia Gateway Control Function	Gere a IMS-MGW, faz adaptação de protocolos de sinalização das redes de comutação de circuitos e redes SIP e pode fazer encaminhamento de chamadas de entrada em redes legadas.	TS 123 002
IP Multimedia Subsystem – Media Gateway Function (IMS - MGW)	Controla acesso a redes de comutação de circuitos, faz transcodificação de sinal das chamadas, implementa mecanismos de cancelamento de eco e fornece serviço de conference bridging	TS 123 002

A *Multimedia Resource Function* é constituída por 2 componentes: o *Multimedia Resource Function Controller* (MRFC) e o *Multimedia Resource Processor Function* (MRPF), como ilustrado na Figura 3.13.

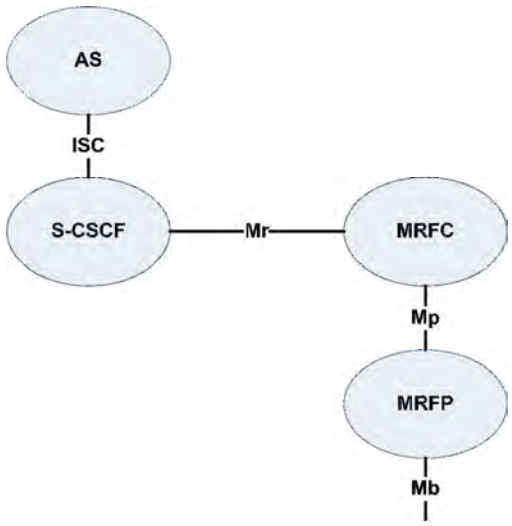

Figura 3.13 – Arquitectura do *Multimedia Resource Function.*

A MRFC possibilita o controlo da MRPF que se encontra no plano de transporte, através de uma interface normalizada, alocando e libertando recursos da rede de core para suportar os serviços, bem como alterando esses mesmos recursos. Interpreta a informação que vem do AS via S-CSCF, como a marcação de conferências e faz a gestão dos recursos da MRFP de acordo com as necessidades criadas pelos pedidos do AF. As funções executadas pelo MRPF são: o controlo da barreira do ponto de referência Mb; o processamento dos fluxos multimédia no caso de transcodificação de áudio ou de análise dos fluxos; a gestão de direitos de acesso a recursos partilhados em ambiente de conferência; e a mistura dos fluxos de entrada no caso de ambiente de

conferência. A Tabela 3.10 resume as características principais dos elementos que compõem a arquitectura do MRF.

Tabela 3.9 - Lista de entidades funcionais da arquitectura do MRF.

ENTIDADE	FUNCIONALIDADE	ESPECIFICAÇÃO
Multimedia Resource Control Function (MRCF)	Interpreta informação que recebe do CSCF e configura MRFP para fornecer recursos na rede do core	TS 123 002
Multimedia Resource Function Processor (MRFP)	Controla fluxos na interface Mb, faz transcodificação de fluxos multimédia e mistura fluxos em ambientes de conferência	TS 123 002

A Tabela 3.10 reúne a informação acerca das interfaces dos elementos do MRF, bem como o protocolo que está na base da comunicação e o documento que define esse mesmo interface.

Tabela 3.10 - Lista de interfaces dos elementos da arquitectura MRF.

NOME	ELEMENTOS	PROTOCOLO	ESPECIFICAÇÃO
Mr	CSCF – MRFC		TS 123 002
Mp	MRFC - MRCF	SIP	TS 29.333
Mb	MRFP -		TS 29.162

3.1.3 TISPAN

O TISPAN desenvolveu uma arquitectura funcional constituída por um conjunto de subsistemas divididos por duas camadas, uma camada designada de camada de serviço e outra designada de camada de transporte, baseada em tecnologia IP (Figura 3.14). A arquitectura modular do TISPAN, permite que novos componentes sejam posteriormente adicionados de acordo com as necessidades, e que sejam integrados componentes desenvolvidos por outros organismos de normalização. Cada uma das camadas é constituída por um conjunto de entidades funcionais, bem como pelas interfaces correspondentes.

A camada de transporte é responsável por fornecer a conectividade de nível 2, conectividade IP e controlo de transporte, sendo composta por: o *Network Attachment SubSystem* (NASS), o *Resource and Admission Control SubSystem* (RACS), além de um conjunto de funcionalidade de transporte.

O NASS é responsável pelo fornecimento de informação de configuração ao terminal do utilizador, fornecendo informação como o endereço IP, o endereço do servidor de nomes e outros dados de configuração. Efectua também a autenticação do utilizador, bem como a autorização dos serviços de acordo com o perfil do utilizador registado.

O RACS é responsável por efectuar controlo de admissão de acordo com o perfil de utilizador e com os recursos disponíveis, por fazer reserva de recursos para os pedidos de recursos aceites e por efectuar a gestão de recursos, efectuar o controlo de gateways e aplicar as políticas de rede.

A camada de serviço é composta por: o *Core* IMS, o subsistema de emulação de PSTN/RDIS (PES), outros subsistemas multimédia e componentes comuns a vários subsistemas tais como: funcionalidades de contabilização, de gestão de perfis de utilizadores e sistemas de gestão de segurança. A componente designada de *Core IMS* corresponde ao sistema IMS normalizado pelo 3GPP e descrito na secção 3.1.2, tendo a versão 1 da arquitectura do TISPAN utilizado a arquitectura proposta na versão 6 do IMS do 3GPP. Na versão 2 da arquitectura NGN [80], o TISPAN utilizou a versão 8 do IMS do 3GPP, para a qual tinha contribuído na definição de outras tecnologias de rede de acesso que não as redes celulares [81], tais como redes de acesso baseadas em *Digital Subscriber Line* (DSL) e redes sem fios locais.

O subsistema de emulação PSTN/RDIS permite que os terminais PSTN acedam á rede NGN através das linhas residenciais.

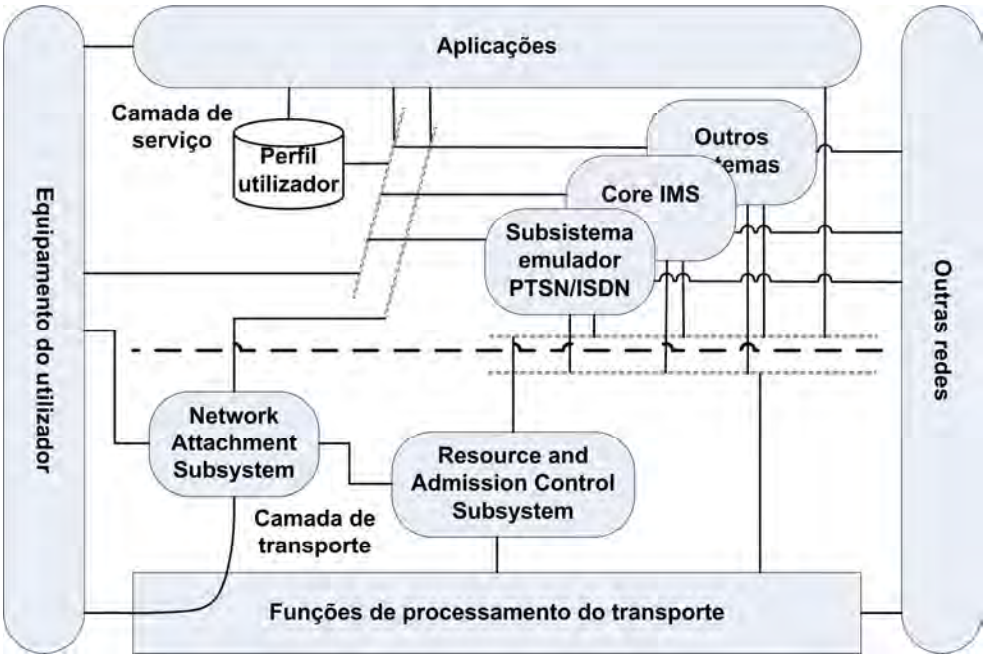

Figura 3.14- Arquitectura da rede NGN do TISPAN [80].

A versão do IMS utilizada pelo TISPAN (Figura 3.15) teve em conta as diferenças existentes nos meios com e sem fios, o que originou algumas diferenças em relação à arquitectura IMS normalizada pelo 3GPP, nomeadamente nos componentes: *Application Server Function* (ASF), a *Inter-Working Function* (IWF) e a *Interconnection Border Control Function* (IBCF).

A ASF é uma entidade capaz de fornecer serviços básicos, ou serviços de valor acrescentado transportados por uma sessão simples. Pode ter um de dois tipos: um ASF do tipo 1 que pode interagir com o RACS; e um ASF do tipo 2 que confia no subsistema de controlo para lhe fornecer uma sessão básica, sobre a qual fornece serviços de valor acrescentado. No caso do ASF do tipo 2, se utilizado com uma plataforma de IMS, a sua funcionalidade corresponde ao AS definido pelo 3GPP.

A IWF é um novo componente que efectua a tradução entre os protocolos utilizados em subsistemas de controlo de serviço e outros protocolos da tecnologia IP, como por exemplo entre o perfil SIP utilizado na rede IMS e outros perfis SIP, ou entre o protocolo SIP e outros protocolos como H.323. Devido às diferenças existentes nas metodologias de contabilização das redes do 3GPP, o TISPAN definiu a IBCF como uma entidade adicional, capaz de desencadear acções de contabilização, encontrando-se conectado ao core IMS.

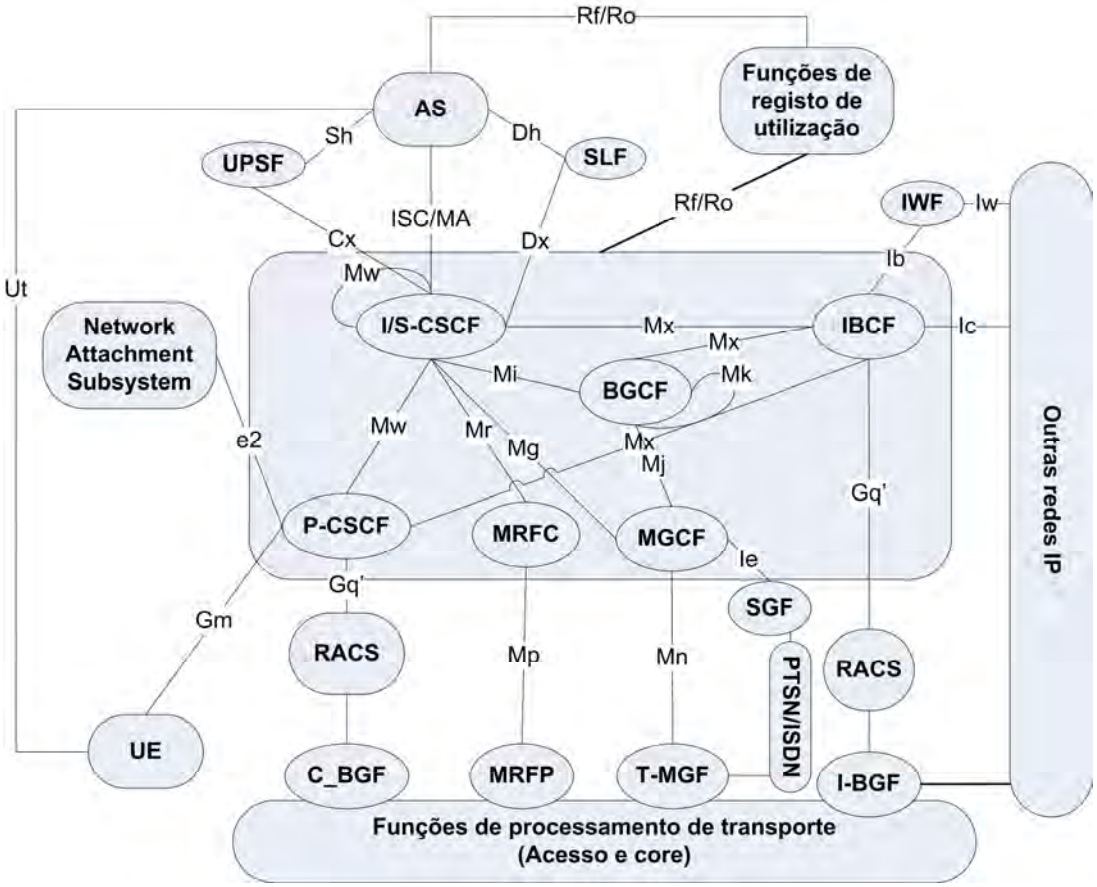

Figura 3.15 - Core IMS da rede NGN do TISPAN.

3.1.4 Outros esforços

DSLForum

O DSLFORUM, agora designado de *Broadband Forum* [66], efectuou melhoramentos na sua arquitectura tendo em vista a evolução ocorrida ao nível dos serviços e tendo em vista a integração com as arquitecturas de NGN existentes.

A plataforma de controlo baseada em políticas para DSL [82] define uma camada de controlo para controlo dinâmico de sessões e controlo da rede em tempo real, bem como suporte de pedidos de recursos de rede da camada de aplicações, por exemplo vindas de servidores IPTV ou de uma plataforma IMS. A especificação da arquitectura não está no entanto concluída, faltando especificar entidades e interfaces.

CableLabs

A arquitectura NGN da *CableLabs* [83], ilustrada na Figura 3.16, inclui uma camada de controlo baseada em políticas e suporta uma grande diversidade de aplicações e serviços, incluindo a plataforma IMS.

O *PacketCable Application Manager* (PAM) mantém informação relativa ao estado das sessões das aplicações e aplica políticas do *Service Control Domain* (SCD) aos recursos de dados através de um *Application Server* como um P-CSCF. O interface *pkt-qos-1* é baseado em tecnologia Web Services e interliga o P-CSCF do IMS ao PAM. Transmite informação de QdS ao nível da sessão que extrai da sinalização SIP. O PAM recebe a indicação de quando reservar os recursos para uma sessão, sendo que opcionalmente pode suportar um conceito semelhante a uma pré-reserva. Adicionalmente aplica as políticas do SCD e traduz os requisitos de recursos das sessões ao servidor de políticas através da interface *pkt-mm-3* que é baseada em COPS.

O servidor de políticas efectua verificação de políticas do *Resource Control Domain* (RCD), por exemplo se a quantidade de recursos se encontra dentro dos limites estabelecidos, se o serviço foi o mais adequado, assegurando que os pedidos respeitam as políticas de rede pré estabelecidas. Depois de passarem os testes do servidor de políticas, os pedidos são encaminhados para o *Cable Modem Termination System* (CMTS) através da interface COPS *pkt-mm-2*.

Depois de receber os pedidos de recursos, o CMTS é responsável por efectuar o controlo de admissão e respectiva alocação de recursos. Finalmente o CMTS instala os fluxos necessários e notifica o modem de cabo que serve o equipamento do utilizador. O modelo de *outsourcing* também é suportado, onde o CMTS envia os pedidos de autorização ao servidor de políticas através de uma interface COPS.

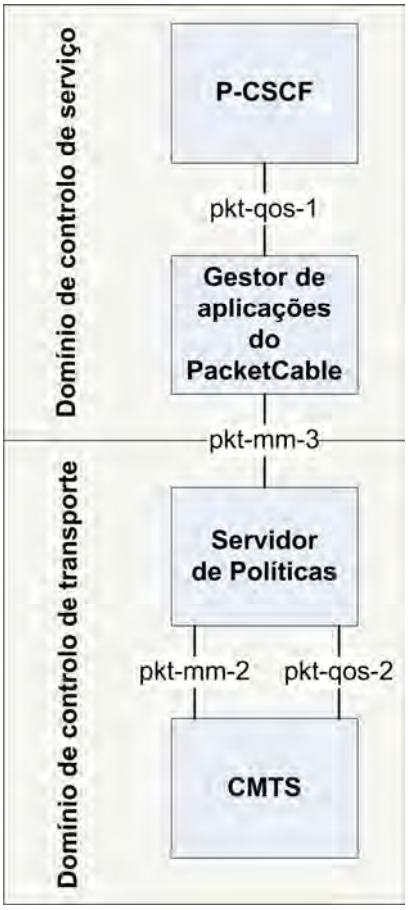

Figura 3.16 – Controlo de admissão baseada em políticas da arquitectura NGN da CableLabs.

3GPP2

O *Third-Generation Partnership Project 2* (3GPP2) definiu uma arquitectura NGN [84] que, tal como o 3GPP, dividiu a rede de core em dois domínios: domínio de comutação de circuitos para suportar serviços baseados em comutação de serviços; e um domínio de comutação de pacotes de forma a suportar serviços baseados de comutação de pacotes. Tal como o 3GPP, o 3GPP2 desenvolveu uma plataforma baseada em tecnologia IP para a disponibilização de serviços multimédia a clientes móveis a que designou de *IP MultiMedia Domain* (MMD) e que seguiu de muito perto a especificação IMS do 3GPP.

O MMD é composto por uma plataforma IMS [85] e por um subsistema de pacotes de dados. O MMD fornece conectividade entre extremos, bem como serviços através da rede de core, e utiliza o IMS com o objectivo de suportar as sessões multimédia.

A Figura 3.17 ilustra simplificadamente a arquitectura IMS proposta pelo 3GPP2. A arquitectura é mesmo muito semelhante à arquitectura IMS do 3GPP; a maioria das entidades possui uma entidade equivalente na plataforma IMS do 3GPP; e as interfaces possuem uma

funcionalidade muito semelhante às suas equivalentes da plataforma IMS do 3GPP. Por exemplo, tal como no IMS do 3GPP, o 3GPP2 utiliza o protocolo SIP para efectuar a gestão de sessões.

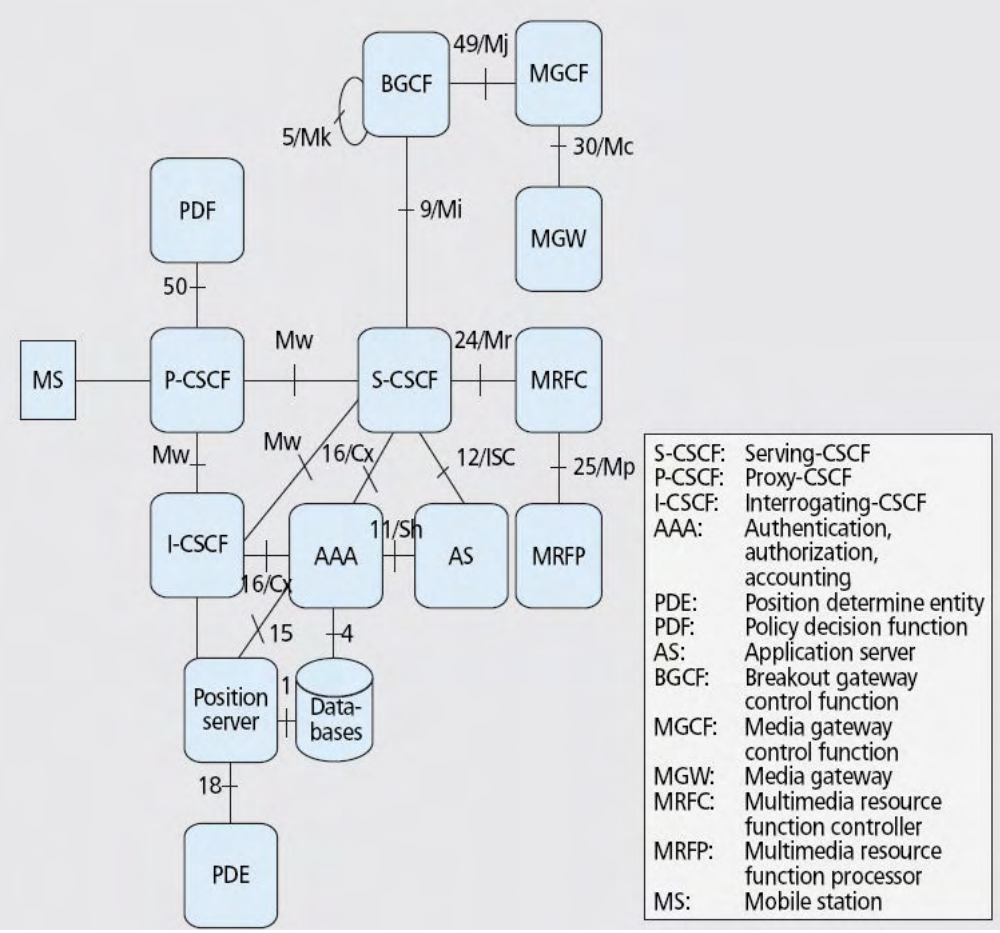

Figura 3.17 - Arquitectura NGN do 3GPP2 [84].

As principais diferenças entre as duas arquitecturas são:

- Gestão de mobilidade: no caso da rede 3GPP2 a mobilidade é implementada com base em Mobile IP; enquanto que no caso do 3GPP é implementada através da implementação de um túnel de *layer-2*, baseado em tecnologia GPRS;
- Versão IP: A plataforma IMS do 3GPP2 suporta tanto IPv4 como IPv6, enquanto que a versão IMS do 3GPP suporta somente IPv6;
- Segurança na rede de acesso: o 3GPP2 permite outros métodos de autenticação que não IPSec, ao contrário do que acontece com a plataforma IMS do 3GPP, podendo no caso do 3GPP2 o equipamento do utilizador negociar através das mensagens SIP com o P-CSCF qual o mecanismo de segurança pretendido;
- Ponto de ligação dos terminais celulares: no caso do 3GPP o GGSN a que um terminal se liga mantém-se ao longo de toda a chamada, independentemente da mobilidade

geográfica a que o terminal seja sujeito; no 3GPP2 o terminal pode mudar de *Packet Data Serving Node* (PDSN), mesmo durante o decorrer de uma chamada;

- Localização do P-CSCF: O P-CSCF do 3GPP está sempre presente na mesma rede que o GGSN; no caso do 3GPP2 o P-CSCF e o PDSN podem não estar na mesma rede;
- Posicionamento geográfico: o IMS do 3GPP2 comunica com elementos de posicionamento geográfico recebendo informação de posicionamento do servidor de posicionamento;
- Repositório de perfis de utilizadores: no 3GPP o HSS é um repositório utilizado tanto pelos domínios de comutação de pacotes, como pelo domínio de comutação de circuitos; o 3GPP2 separa as funcionalidades de do HSS do 3GPP num servidor de AAA e outros repositórios.
- Serviços CAMEL: não são suportados na rede IMS do 3GPP2.

3.1.5 Sumário das características das arquitecturas NGN

A corrente secção sumaria as características comuns das várias arquitecturas descritas nas secções anteriores, agrupadas em características relacionadas com a infra-estrutura da rede, com os serviços disponibilizados, com os terminais de rede e com a plataforma de gestão.

A especificação NGN do 3GPP influenciou, graças à boa recepção obtida pela plataforma IMS, a maioria das arquitecturas de rede NGN estudadas. No caso do TISPAN tem havido um esforço muito considerável de desenvolvimento de suporte para outras tecnologias de acesso à rede da plataforma IMS de forma a finalmente atingir uma convergência entre as redes móvel e fixa. Por parte do 3GPP2 tem havido um acompanhamento das propostas do 3GPP, com alterações à arquitectura muito restritas. Apesar de não terem seguido de tão perto a arquitectura do 3GPP, as propostas do *ClableLabs* e *Broadband Forum*, mostram também semelhanças consideráveis com a proposta do 3GPP.

Apesar das semelhantes em termos arquitecturais, a nomenclatura utilizada por cada uma das organizações é diferente, tanto em termos de nomes das entidades funcionais, como de nomes das suas interfaces.

A arquitectura ITU-T é a mais abrangente, em termos de âmbito de utilização: especifica mecanismos de gestão da rede de acesso e da rede de core. No caso da rede TISPAN, o controlo de recursos da rede é efectuado na rede de acesso e nos elementos de fronteira com a rede de core. Todas as outras arquitecturas aqui descritas limitam o controlo de recursos à rede de acesso.

Apesar plataforma IMS ser dita de "agnóstica em relação à tecnologia de rede de acesso" e de as arquitecturas de rede aqui descritas utilizarem essa plataforma, a maioria das propostas limita-se a contemplar tecnologias de redes de acesso originárias das suas áreas de interesse (*e.g.*:,

3GPP contempla tecnologias de acesso para redes celulares, *Broadband Forum* contempla acesso DSL, etc.). Só as arquitecturas do ITU-T e do TISPAN são verdadeiramente flexíveis permitindo qualquer tipo de tecnologia de rede de acesso.

Uma característica comum a todas as arquitecturas de redes é que baseiam os mecanismos de controlo de admissão no paradigma de gestão baseada em políticas, utilizando esquemas de regras para definir critérios de admissão de novos fluxos. Na sua maioria os esquemas de controlo de acesso são dinâmicos, sendo excepções as propostas da *PacketCable* e do *Broadband Forum*.

A Tabela 3.11 resume as características gerais das arquitecturas de rede NGN descritas anteriormente.

Tabela 3.11 - Comparação de características das redes NGN.

INICIATIVA	REGIÃO DE CONTROLO	TECNOLOGIA DE TRANSPORTE	TIPO DE CONTROLO	PORMENOR
ITU-T	Redes de acesso e core	Independente da tecnologia	Dinâmico	Controlo de admissão ao nível das chamadas e controlo de recursos através de controlo de agregados de tráfego. Controlo de QdS tanto para rede de acesso como para a rede de core.
TISPAN	Rede de acesso e fronteira com a rede de core	Independente da tecnologia	Dinâmico	Controlo ao nível das chamadas. Gestão de recursos na rede de acesso e na fronteira com a rede de core.
3GPP	Rede de acesso	Rede celular	Dinâmico	Controlo de sessões e de serviços através da plataforma IMS.
3GPP2	Rede de acesso	Rede celular	Dinâmico	Controlo de sessões e de serviços através da plataforma IMS.
PacketCable	Rede de acesso	Rede cabo	Estático e dinâmico	Controlo de sinalização de estabelecimento de chamadas e recursos de transporte da rede de acesso.
Broadband Forum	Rede de acesso	Rede DSL	Estático	Controlo de QdS baseado em configuração Diferenciação de serviços baseada em arquitectura *DiffServ*.

Em termos de integração com a plataforma de gestão de serviços, todas as arquitecturas se integram com a plataforma IMS e suportam a recepção de pedidos de recursos da plataforma de serviços através de um pedido do CSCF.

Todas as arquitecturas implementam os mecanismos de controlo de admissão recorrendo a elementos decisores e a elementos que implementam na rede as decisões dos primeiros. No caso da arquitectura do 3GPP são propostas entidade decisora e executora únicas; as outras arquitecturas recorrem à utilização de mais do que uma entidade.

A Figura 3.18 ilustra a distribuição das diversas entidades, pelas diversas camadas das várias arquitecturas estudadas, bem como o nome das diversas interfaces propostas.

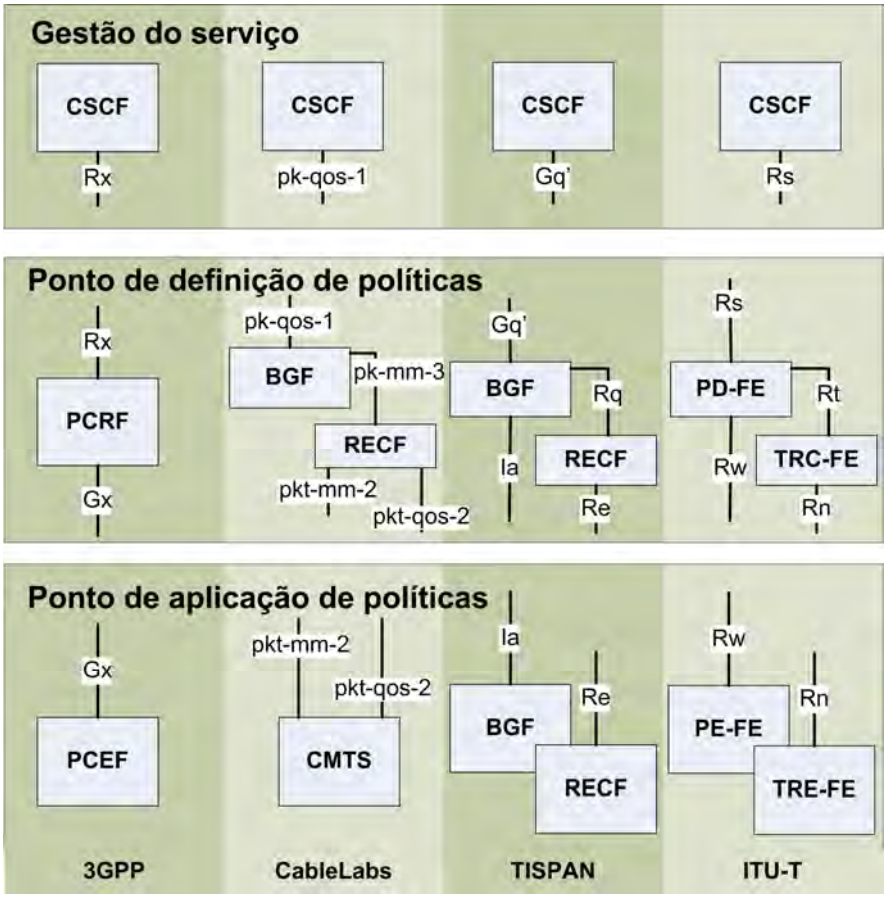

Figura 3.18 - Comparação de diversos pontos da arquitectura.

Analisando as interfaces entre as entidades propostas pelas várias entidades normalizadoras, verificamos que o protocolo Diameter é o mais utilizado, especialmente na proposta do 3GPP onde as últimas versões da arquitectura têm vindo a reutilizar na maioria das interfaces o suporte de comunicação baseado em Diameter [52]. A arquitectura *CableLabs* mantém a comunicação com a plataforma de gestão de serviços através de uma interface Web Services e a comunicação entre as entidades envolvidas no controlo de admissão, tal como a *Broadband Forum*, através de uma interface baseada em COPS.

A Tabela 3.12 enumera um conjunto de características das interfaces das entidades envolvidas no controlo de admissão.

Apesar das diferenças anteriormente referidas, existem grandes semelhanças entre as redes propostas, que a seguir se listam agregadas nas categorias de: infra-estrutura de rede, arquitectura dos terminais, serviços e gestão da rede e dos sistemas.

No que respeita à infra-estrutura das redes:

- Redes de acesso heterogéneas IPv6 com integração de tráfego redes de diferentes tecnologias, entre as quais: IEEE 802.11, 802.15, 802.16, tráfego DVB, redes de acesso

celulares como o TD-CDMA; permitindo assim uma ampla cobertura de rede de acesso sem fios;

- Suporte de QdS com diversidade de serviços de transporte, diferentes prioridades, diferentes preços, bem como a utilização de mecanismos de controlo de admissão de novos fluxos;
- Suporte de mobilidade transparente entre redes de acesso e entre redes de diferentes operadores, e mobilidade de utilizadores entre diferentes terminais;
- Utilização de redes não estruturadas e a sua integração com redes estruturadas e utilização de redes móveis em cenários relacionados com transportes públicos;
- Criação de redes de sensores que permitirão às várias entidades da rede a adaptação às preferências dos utilizadores; e aos utilizadores conhecer as facilidades que a rede lhe pode oferecer em cada local.

No que respeita às arquitecturas dos terminais:

- Terminais com múltiplas interfaces de diferentes tecnologias com a possibilidade de troca de tecnologia de acesso, mediante a variação das condições de rede ou condições de utilização;
- Terminais inteligentes com a possibilidade de se adaptarem às preferências do utilizador e com agentes que lhe permitirão tomar decisões em nome do utilizador, tais como a escolha da rede de acesso através de critérios definidos pelo próprio utilizador em função das condições de acesso e utilização, numa estratégia de escolha do melhor serviço ou da melhor ligação;
- Terminais com interfaces gráficos melhorados e a possibilidade de utilização de serviços de áudio e vídeo; permitindo uma interacção com o utilizador através da medição de dados biométricos tais como a leitura de sinais vitais;
- Diminuição de tamanho e peso dos terminais e o consequente aumento de portabilidade e integração com o corpo humano e com o vestuário.

No que respeita aos serviços:

- Integração de serviços de múltiplos fornecedores devido aos ambientes federados criados pelos operadores de comunicações;
- Ampla utilização de serviços de voz em IP (VOIP) com a criação de diversas classes de serviço para o transporte de voz;
- Criação de serviços multimédia que permitirão a utilização mais comum de processos de comunicação entre utilizador e uma máquina, ao contrário da comunicação entre utilizadores como é comum actualmente;

- Serviços de localização que permitirão ao utilizador conhecer o meio em seu redor e permitirão à rede adaptar-se à chegada do utilizador, eventualmente notificar os utilizadores da presença uns dos outros;
- Utilização de serviços de rede com diferentes qualidades e diferentes requisitos de largura de banda;
- Grande variedade de serviços de transporte com a existência de serviços assimétricos, existindo ainda serviços bidireccionais e unidireccionais. Para além de serviços de transporte *unicast*, deverão ainda ser implementados serviços de transporte *broadcast* e outros *multicast*;
- Gestão de utilizadores com suporte de autenticação, autorização de serviços baseados no perfil de utilizador, com registo de utilização, possibilidade de consulta da utilização efectuada e contabilização do custo da utilização;
- Implementação de mecanismos que possibilitem registo único na rede, permitindo acesso a múltiplos serviços de diferentes entidades;

No que respeita à gestão da rede e dos sistemas que a integra:

- Gestão integrada da rede independentemente das tecnologias e independência entre a gestão de recursos e a gestão de serviços;
- Criação de plataformas abertas para a integração de operadores de serviços com a infra-estrutura do operador.

Tabela 3.12 – Características das interfaces entre as entidades envolvidas no controle de admissão.

CARACTERÍSTICA	3GPP R5/6	3GPP R7	CABLELABS	TISPAN	3GPP2	ITU-T
PDP	PDF	PCRF	PAM PS	RACS (S-PDF, A-RACF)	PCRF	RACF (PD-PE, TRC-FE)
PEP	PEP	PCEF	CMTS	BGF RECF	PCEF	PE-FE TRE-FE
Interface MM	Gq <Diameter>	Rx <Diameter>	pkt-qos-1 <WebServices>	Gq' <Diameter>	Rx <Diameter>	Rs <Diameter>
Interface rede	Go <COPS>	Gx <Diameter>	pkt-qos-2 <CPD> pkt-mm-2 <COPS>	Ia<H248> Rq<Diameter>	Gx <Diameter>	Não especificado
Push mode	Não	Não	Sim	Sim	Não	Sim
Pull mode	Sim	Sim	Sim	Sim(R2)	Sim	Sim

3.2 Tecnologias de gestão utilizadas em redes NGN

A actual secção descreve as tecnologias mais relevantes que são utilizadas em redes NGN, nomeadamente as relacionadas com a gestão da rede e de QdS.

3.2.1 Gestão de qualidade de Serviço

Tem-se assistido na última década a uma massificação da utilização do protocolo IP para transporte de múltiplos tipos de tráfego, como transferência de dados, transporte de voz ou *streaming* de vídeo ou de áudio. Esses tipos tão diversos de tráfego têm também requisitos de largura de banda, de atraso de chegada e de perda dos pacotes muito diversos. Por exemplo uma aplicação de transferência de dados será muito tolerante a um atraso na chegada dos pacotes, mas uma aplicação de VOIP com certeza não o será. O valor associado a cada um dos serviços que utilizam a infra-estrutura de rede não é também o mesmo: o preço de um serviço de voz ou de um serviço de vídeo-conferência é sempre muito mais caro do que um serviço de acesso à web em qualquer fornecedor de serviços de comunicações.

O aumento de tráfego produzido pelo crescente número de utilizadores e de serviços de rede cria também novos problemas: as capacidades das ligações são limitadas e com aumento de tráfego tendem a ficar saturadas. A saturação das ligações e dos elementos da rede faz aumentar os atrasos e aumenta as probabilidades de que os pacotes sejam descartados numa das filas dos *routers*. A solução para aliviar a infra-estrutura de rede da sobrecarga é a colocação de novos links de dados com novos elementos para efectuar a condução dos pacotes de dados através da rede, o que implica enormes investimentos financeiros.

O carácter democrático de entrega dos pacotes de cada um dos serviços numa base de melhor esforço, bem como a tarifação de todos os serviços ao mesmo preço não ajuda à rentabilização dos investimentos financeiros que os operadores necessitam de fazer de forma a melhoras as capacidades de transmissão das redes de comunicações. Tendo em conta que os recursos de rede são partilhados por todos os serviços e que esses serviços tem diferentes preços, a solução para um operador consiste em efectuar uma diferenciação do tratamento dado aos pacotes de diferentes serviços, de acordo com o valor que cada um desses serviços para as receitas do operador.

Qualidade de serviço consiste em efectuar a diferenciação do tráfego de acordo com o serviço a que pertence o pacote, com o seu destino ou a sua origem. A contractualização do serviço prestado ao cliente é caracterizada por um conjunto de condições, entre as quais os diferentes preços e os parâmetros que caracterizam o tratamento que os pacotes recebem pela infra-estrutura de rede do operador, o que também se designa por garantia QdS. A definição de QdS pode ser feita em termos tão abstractos como "*conjunto de parâmetros do serviço que garante a satisfação do utilizador*". No âmbito de uma rede IP, os parâmetros de QdS que normalmente se pretendem controlar são fundamentalmente a largura de banda, o atraso e a sua variância.

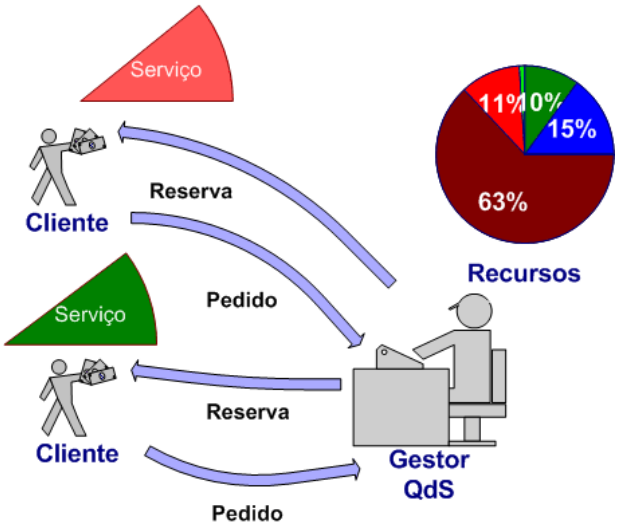

Figura 3.19 - Conceito de qualidade de serviço.

Com vista à resolução dos problemas criados pelo aumento de tráfego numa rede e à criação de mecanismos que possibilitassem o fornecimento de garantias de QdS, o IETF criou um grupo de trabalho que definiu um modelo de QdS chamado Serviços Integrados (*IntServ*). Este modelo de QdS apesar de fornecer garantias de QdS aos fluxos admitidos para todo o percurso entre a origem e o destino, tem um sério problema de escalabilidade, o que o torna pouco adequado para redes de core [86]. Foi então criado um novo grupo de trabalho pelo IETF, com vista a criar um novo modelo de QdS que não sofresse dos problemas de escalabilidade, a que se chamou Serviços Diferenciados (*DiffServ*). Este modelo foi melhor recebido pelos operadores e já não sofre dos problemas de escalabilidade do modelo anterior. Mas para fornecer garantia de QdS entre extremos da rede, necessita de mecanismos de controlo de admissão. Quando as condições de sobrecarga dos elementos de rede não permitam o serviço de um novo fluxo, este não deverá ser admitido, mas os fluxos anteriormente admitidos continuarão a ser servidos de acordo com os parâmetros de QdS a eles associados.

Na subsecção seguinte são descritos diferentes modelos de QdS, bem opções de interligação entre deferentes modelos.

Integrated Services

Em resposta à procura crescente de mecanismos de QdS, o IETF criou o *Integrated Services* (*IntServ*) *Working Group*. Esta arquitectura foi desenvolvida para optimizar a utilização dos recursos de rede para aplicações que requerem limites do tempo de atraso e para as quais o tempo de entrega dos pacotes tem uma importância crítica, como aplicações multimédia em tempo real. Este tipo de aplicações não se adequa com o tráfego *best-effort* devido aos atrasos no

encaminhamento e às perdas de informação quando ocorre congestionamento na rede. Na arquitectura *IntServ* [87] cada pacote é associado a um fluxo definido pelos seus endereços de origem e de destino e pelo número do porto.

O *IntServ* permite três tipos de serviços distintos, a seguir descritos: *best-effort*, *guaranteed service* e *controlled load*. O serviço *best-effort* (ou ASAP como também é conhecido) é usado por tráfego sem qualquer garantia de QdS. Neste tipo de serviço os pacotes são entregues logo que seja possível, sem qualquer garantia. O atraso dos pacotes é indeterminado à partida, pois não são reservados quaisquer recursos e por isso o atraso estará dependente da sobrecarga da rede naquele instante. Também não oferece garantia de entrega dos pacotes, uma vez que em caso de sobrecarga os *routers* fazem descarte dos pacotes, começando pelos pacotes de *best-effort*.

Num cenário de pouca sobrecarga da rede estes pacotes são entregues no destino sem perdas e com pequeno atraso. Quando a sobrecarga dos elementos da rede aumenta, os pacotes passam a ser entregues com atrasos maiores, podendo ser descartados por um dos elementos da rede, se a quantidade de pacotes a transmitir for muito elevada.

As aplicações mais indicadas para este tipo de serviço são aquelas em que o atraso na chegada dos pacotes é tolerado, de que são exemplos Telnet, FTP, HTTP, etc.

O Serviço *Guaranteed Service* [4] (serviço garantido) fornece uma largura de banda entre extremos garantida sem perda de pacotes para fluxos que respeitem o perfil de QdS, sendo semelhante ao de uma linha comutada virtual. A sua grande vantagem é que é possível definir um atraso máximo para os pacotes na rede, não existindo descarte nas filas dos *routers* da rede.

É especialmente concebido para aplicações com requisitos específicos de largura de banda com intolerância, quer à degradação do nível de largura de banda disponível, quer à perda de pacotes. As características do tráfego são sujeitas a análise, de modo a verificar a concordância com as condições definidas; O tráfego não conforme é tratado como *best-effort*, mas podendo acontecer que seja descartado.

O serviço *controlled load* [5] (ou *predictive service* como também é conhecido) não apresenta garantias quantitativas, ao contrário do serviço *guaranteed service*. A garantia que este tipo de serviço apresenta é a de que o tráfego deste tipo de serviço não sofrerá degradação significativa com o congestionamento, como o que acontece para tráfego *best-effort*. Em termos de comportamento é semelhante ao serviço *best-effort* em redes pouco congestionadas. Os *routers* que implementem este serviço devem verificar se as características do tráfego estão de acordo com as condições definidas, de modo a tratar o tráfego não conforme como *best-effort* ou até para o descartar. Assim, este serviço é vocacionado para aplicações que tolerem alguma degradação da largura de banda e ocorrência de atraso, como aplicações de tempo-real que sejam adaptativas. Um elemento de rede *IntServ* pode ser dividido em várias entidades funcionais. Os elementos internos

podem ser identificados como: *classificador de pacotes* que identifica e selecciona o tipo de serviço de cada pacote; o *escalonador* que selecciona os pacotes das diversas filas de espera, de modo a que estes sejam servidos cumprindo os requisitos de QdS requisitada; o *controlador de admissão* que determina quais os pedidos de reserva que podem ser aceites, de modo a que esse serviço possa ser concedido sem pôr em causa o serviço dos restantes fluxos já autorizados; o *protocolo de sinalização* que processa as mensagens recebidas e entrega-as ao controlador de admissão; o processo de *routing* que consiste no processo de encaminhamento existente no *router* que determina qual o próximo nó para o fluxo em questão; a *política de controlo* que define um conjunto de políticas que determinam o comportamento do elemento de rede;

Como se pode deduzir da Figura 3.21, a arquitectura *IntServ* supõe que possa existir mais do que um elemento de rede entre o originador e o destinatário do fluxo e que existem dois fluxos independentes: um para a sinalização que a arquitectura *IntServ* necessita, e outro de informação a ser transmitido entre o originador e o destinatário. Na figura estes dois fluxos estão separados pelas linhas a tracejado.

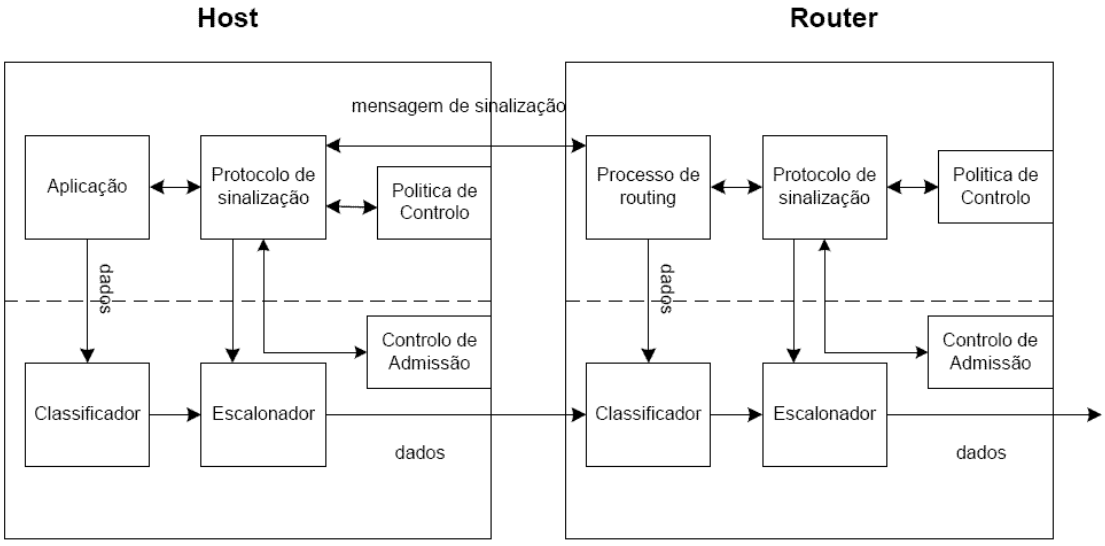

Figura 3.20 - Funcionamento dos nós de rede *IntServ*.

Para que os pacotes de um fluxo possam ser tratados com uma determinada qualidade de serviço é necessário que estes sejam identificados. Depois da identificação dos pacotes, estes são mapeados para uma classe de serviço, sendo encaminhados para a respectiva fila. A identificação da classe e o seu mapeamento para a classe de tráfego a utilizar são feitos pelo classificador de pacotes. Sendo uma classe uma abstracção de um *router* específico, um pacote pode ser mapeado em diferentes *routers* para diferentes classes. No classificador de pacotes o importante é garantir

que a classe onde o pacote foi mapeado tenha um tratamento tal que o pacote obtenha a qualidade de serviço que necessita.

Normalmente o classificador usa a informação proveniente do cabeçalho IP do pacote: endereços de origem, de destino e do cabeçalho do protocolo da camada acima: protocolo e número de porto. É ainda possível que o classificador procure informação nas camadas acima, no cabeçalho da camada de aplicação. Esta implementação é complexa, pois requer a análise dos cabeçalhos dos pacotes de várias camadas protocolares, o que é muito dispendioso em termos de tempo. O escalonador de pacotes é a entidade que gere a entrada em serviço dos diversos pacotes das várias filas do *router*, de acordo com a classe a que cada fila pertence. Tem que assegurar que o serviço de cada pacote está de acordo com os parâmetros de QdS definidos. Existem vários algoritmos de escalonamento que podem ser usados pelo escalonador, como prioritização estrita, *Round-Robin*, *Fair-Queuing*, *Weight-Fair-Queueing*.

A qualidade de serviço em *IntServ* assenta no princípio dos *routers* se comprometerem a reservar os recursos para que os fluxos os possam usar. Para que esse princípio seja respeitado, é necessário que os recursos sejam previamente requisitados e que o *router* os reserve para esse uso. Para que o *router* se comprometa a fazer a reserva, é necessário que este possa fazer uma análise do seu estado de ocupação e da disponibilidade de um recurso ser disponibilizado. O pedido deverá ser recusado se não existirem recursos e qualquer admissão só pode ser feita se esse serviço puder ser prestado sem prejudicar o serviço dos fluxos que entretanto já tenham sido admitidos. Cabe ao classificador policiar as propriedades dos fluxos e determinar se os pacotes de um fluxo estão de acordo com a reserva efectuada e se a largura de banda do mesmo não está a ser excedida. No caso de a política escolhida para aplicar aos pacotes que não respeitem as condições da reserva que foi feita ser o descarte, cabe ao escalonador executar esta acção.

Differentiated Services (*DiffServ*)

Numa tentativa de colmatar as dificuldades de escalabilidade existentes na arquitectura *IntServ*, o IETF criou em meados de 1997 o *Differentiated Services Working Group*. Este grupo definiu novos comportamentos de encaminhamento dos *routers* (*hops*), chamados *per-hop behaviors* (PHB). Estes comportamentos descrevem a influência do *router* num fluxo de pacotes, o que se traduz no serviço disponibilizado a um conjunto de fluxos com o mesmo serviço, processando agregados de informação.

Foi definido um número limitado de serviços a fornecer pela rede e uma arquitectura simples para os nós do core, de modo a alcançar os objectivos de escalabilidade da rede, mantendo a diferenciação de tratamento adequada, baseada na marcação existente nos marcadores. Assim, de acordo com o que é especificado em [88], todo o tráfego que entre numa rede *DiffServ* é

classificado e condicionado nas fronteiras da rede, onde é atribuído a diferentes agregados e depois é processado internamente por agregado.

O trabalho do IETF focou-se na altura em dois tipos de serviços: o *Assured Service*, também chamado de *Assured Forwarding Service*, e *Premium Service*, ou *Expedited Forwarding Service*.

Como serviços diferenciados foram definidos:

- *Best-Effort Service(BE)*. É o tipo de serviço em que assenta a Internet actualmente. Não tem qualquer diferenciação de QdS. Todos os utilizadores podem tentar dispor dos recursos que a rede tem sem qualquer discriminação. Para este serviço definiu-se o code point 000000 (default code point).
- *Expedited Forwarding Service* (EF). É também designado como Premium Service e é entendido como uma linha alugada virtual. Neste serviço a Largura de Banda não pode ser excedida, apesar de poder ser total ou parcialmente usada. Neste serviço o cliente não deve sentir a influência da possível simultaneidade de utilização da rede por outros utilizadores. O codepoint recomendado é o 101110.
- *Assured Forwarding Service* (AF). É normalmente também conhecida como *Assured Service*. Fornece uma Largura de Banda aos utilizadores, apesar de não garantir a sua possibilidade de utilização. Os seus pacotes são marcados com uma prioridade mais alta do que os pacotes de BE e a rede funciona de modo que, em condições de congestionamento da rede, os fluxos deste serviço sintam sempre uma menor redução de largura de banda do que os utilizadores do serviço BE.

Existem quatro classes, cada uma com três níveis de precedência de descarte. Cada uma é atendida separadamente das outras, tendo a sua própria fila de espera. Para que se pudesse diferenciar os pacotes e criar um comportamento diferenciado, o IETF propôs que fosse usado um byte do cabeçalho do protocolo IP. Tanto no IPv4 (campo ToS), como no IPv6 (campo Class) existe um byte que suporta QdS. O campo proposto chama-se *Differentiated Service* (DS) e foi definido de modo a manter compatibilidade com esse byte. O *Differentiated Service Code Point* (DSCP) é assim inserido no campo Class (IPV6) ou no campo TOS (IPv4). O DSCP define qual o serviço que o pacote recebe na rede, bem como o tratamento que deve ter por parte dos *routers*. Vários DSCP podem ser agrupados e receber o mesmo PHB nos nós DS. Os pacotes de um fluxo têm o mesmo valor de DSCP.

Um nó *DiffServ* pode ser representado por uma combinação de quatro componentes cuja relação pode ver-se pelo esquema da Figura 3.21. Quando o pacote chega ao classificador é-lhe atribuída uma classe de acordo com a categoria do serviço a prestar. Depois o classificador envia o pacote para o *condicionador*, que inclui um *medidor*, um *marcador*, um *formatador* e um

descartador. As linhas contínuas representam o percurso dos pacotes, enquanto as linhas a tracejado representam sinais de controlo enviados para os componentes do condicionador.

As características de cada elemento são as seguintes:

- *Classificador*: pertencer a um de dois tipos classificador de *Behavior Aggregate* (BA) que escolhe os pacotes só com base nos *codepoints*, e o classificador *Multi-Field*, que escolhe com base em outra informação, que pode ser os endereços de origem e destino, o ID do protocolo, os portos ou outra;
- *Medidor:* mede durante algum tempo os parâmetros de um fluxo de pacotes e compara esses dados com o perfil de tráfego especificado no *Traffic Conditioning Agreement*. Depois passa informação aos outros blocos de condicionamento, para que saibam da concordância dos parâmetros de um fluxo com o perfil correspondente;
- *Marcador:* adiciona ou altera o valor do campo DS ao pacote, juntando-o aos pacotes de um determinado serviço;
- *Formatador:* é uma entidade que faz armazenamento de pacotes e que é normalmente controlado pelo medidor. Atrasa um ou mais pacotes de um fluxo, para que este respeite as condições do perfil de tráfego.

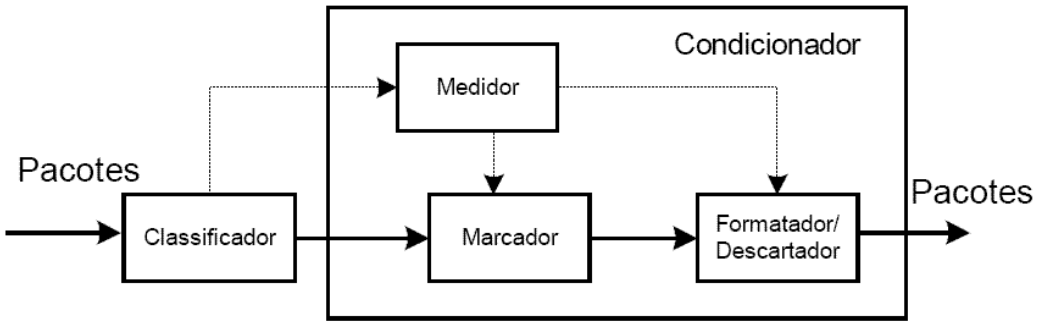

Figura 3.21 - Esquema interno de um nó *DiffServ*.

Integração de diferentes arquitecturas de QdS

A arquitectura *IntServ* tem sérios problemas de escalabilidade devido ao facto de necessitar de manter o estado das reservas válidas não sendo por isso uma opção válida para *routers* do core de uma rede. É no entanto muito eficaz no que toca às garantias de QdS que fornece. No caso da arquitectura *DiffServ* os problemas de escalabilidade foram resolvidos, só que as garantias de QdS fornecidas pelas soluções baseadas em *DiffServ* são relativas a outro tráfego. A arquitectura *DiffServ* não dá qualquer certeza acerca do tratamento do tráfego, só de uma diferenciação entre o tráfego pertencente a diferentes classes de serviço.

As redes de comunicações MPLS continuam a ser hoje em dia muito utilizadas, principalmente nas redes de core dos operadores graças em parte à eficiência de processamento dos diferentes pacotes através da análise das etiquetas MPLS, cujo processo foi anteriormente descrito. Apesar de utilizada nas redes de core dos operadores não tem grande utilização nas redes de acesso, pelo que o tráfego MPLS tem que ser inserido em redes sem suporte de troca de etiquetas. Perante este cenário onde as várias arquitecturas de QdS são utilizadas nas redes de um mesmo operador tornou-se necessário desenvolver mecanismos de integração das diferentes arquitecturas [89].

Apesar de permitir aproveitar as vantagens de cada uma das arquitecturas pela integração das arquitecturas, criam-se alguns desafios com que é preciso lidar: é necessário adaptar as classes de serviço de cada uma das arquitecturas de modo a que o tráfego vindo de uma delas pertencente a uma classe de serviço seja transportado pela rede da nova arquitectura com uma classe que seja equivalente à anterior; a sinalização utilizada (implícita ou explicita) nas diferentes arquitecturas é diferente e tem que ser recreada sempre que o tráfego entra dentro de uma rede baseada em outra arquitectura.

A RFC 2998 [86] propõe uma plataforma de suporte de *IntServ* em redes *DiffServ*.

3.2.2 Arquitectura de gestão de redes NGN

O 3GPP define um conjunto de requisitos para as plataformas de gestão das redes em [90] e [91], de onde destacamos: a possibilidade de gestão de equipamento de diferentes fabricantes, a minimização da complexidade e dos custos da gestão, a comunicação entre entidades através da utilização de interfaces normalizados, o fornecimento de mecanismos de configuração flexíveis para rápido desenvolvimento de serviços, o fornecimento de funcionalidades de gestão de falhas e gestão de segurança, a interoperabilidade entre operadores para troca de informação de gestão e contabilização, a reutilização de normas e tecnologias relevantes, e a existência de mecanismos de contabilização e facturação flexíveis que suportem contabilização da utilização entre redes.

A arquitectura da plataforma de gestão proposta pelo 3GPP identifica um conjunto de entidades como elementos de rede (*Network Elements* - NE), gestores de elementos (*Element Manager* - EM), gestores de domínio, (*Domain Manager* - DM), gestores de rede (Network Manager - NM) e sistemas empresariais (Enterprise System - ES), bem como identifica um conjunto de possíveis interfaces [90]:

- ***Interfaces do tipo 1***: interfaces entre os NE e o DM;
- ***Interfaces do tipo 2***: interligam os DM aos NM do mesmo operador, ou interligam o NM ao EM que existe em certos NE;
- ***Interfaces do tipo 3***: interligam NM aos ES do seu operador;
- ***Interfaces do tipo 4***: interligam NMs do mesmo operador;

- ***Interfaces do tipo 4a***: interligam DMs do mesmo operador;
- ***Interfaces do tipo 5***: interligam ES ou NM de operadores diferentes;
- ***Interfaces do tipo 5a***: interligam NM de operadores diferentes;

São ainda designados de interfaces do tipo *Itf-P2P* os interfaces para entidades do mesmo tipo, tais como os interfaces do tipo *4a* e *Itf-N* e os interfaces que interligam os NM aos DM e EM. A Figura 3.22 ilustra o modelo de referência de gestão do 3GPP [90], onde se encontram ilustradas as entidades e respectivas interfaces. Para as interfaces do tipo 1 são propostos protocolos de comunicação como SNMP, COPS IIOP e SOAP e são aconselhados modelos de dados independentes dos protocolos de comunicação utilizados na implementação das interfaces.

Para as interfaces do tipo 3 não são feitas propostas para a comunicação, uma vez que se considera que os sistemas de gestão empresariais estão fora do âmbito de normalização do 3GPP e porque estão intimamente ligados à estratégia de gestão empresarial dos operadores. É no entanto realçada a importância de uma estreita ligação entre a gestão empresarial do operador com a gestão da infra-estrutura que permite a implementação dos serviços fornecidos por esse operador, o que acontece com várias arquitecturas de gestão como a *enhanced Telecom Operations Map*, TMN ou DEN-ng.

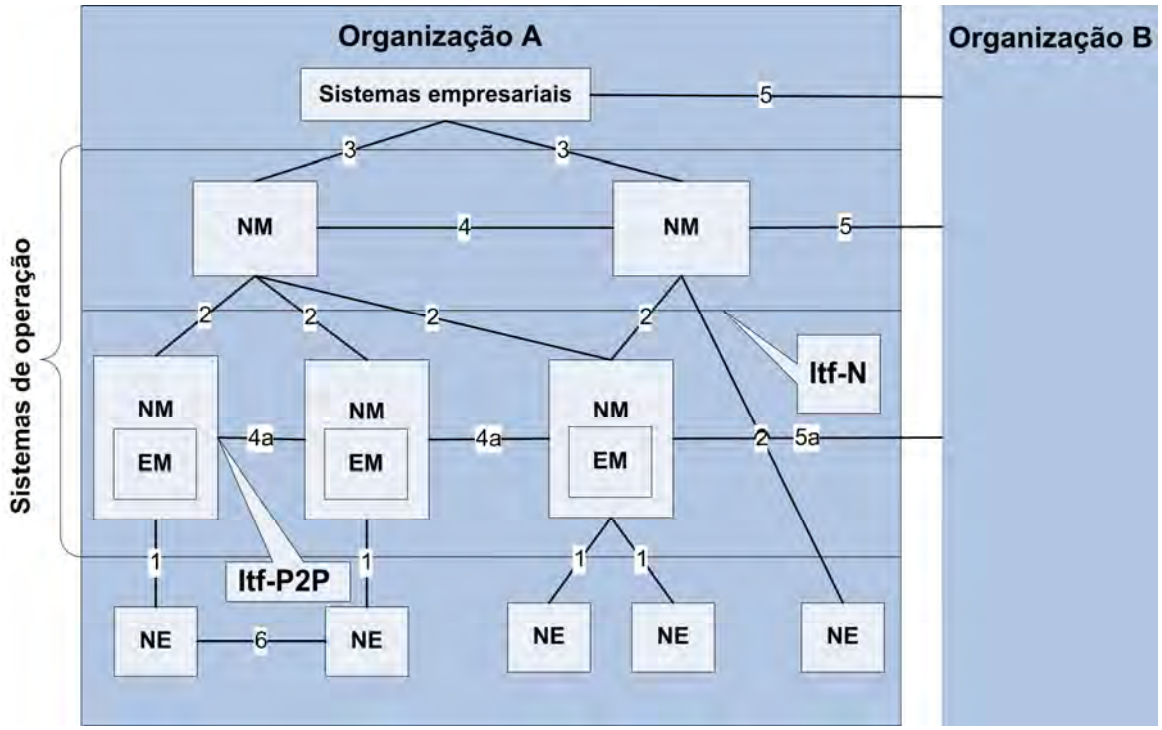

Figura 3.22 - Modelo de referência de gestão [90].

No que respeita às interfaces do tipo 4 não são definidos quaisquer requisitos uma vez que é identificada a necessidade de rever os requisitos que este tipo de interface tem sobre as interfaces

do tipo *4a*. Para as interfaces do tipo *4a* deve ser reutilizada tecnologia semelhante à tecnologia utilizada no desenvolvimento das interfaces do tipo 2.

A comunicação entre entidades que utilizam interfaces do tipo 5 está associada ao suporte de mobilidade entre operadores, como por exemplo ao suporte de *roaming* e ao acesso a serviços fornecidos por outras redes de outros operadores, não sendo no entanto definido qualquer requisito para as interfaces desse tipo.

As áreas funcionais de gestão identificadas pela documentação de gestão do 3GPP são: gestão de desempenho, gestão de mobilidade, gestão de fraudes, gestão de falhas, gestão de segurança, gestão de software, gestão de configuração, gestão de contabilização, gestão de subscrições, gestão de QdS e gestão dos equipamentos dos utilizadores.

A arquitectura de gestão de QdS proposta em [90] é uma arquitectura distribuída (Figura 3.23) que se encontra dividida em 3 camadas: a camada dos NE, a camada dos gestores dos elementos (*Element Management Layer* - EML) e a camada de gestão de rede (*Network Management Layer* - NML). Nessa arquitectura genérica são ainda definidas duas áreas funcionais: o fornecimento das políticas de QdS e a monitorização de QdS.

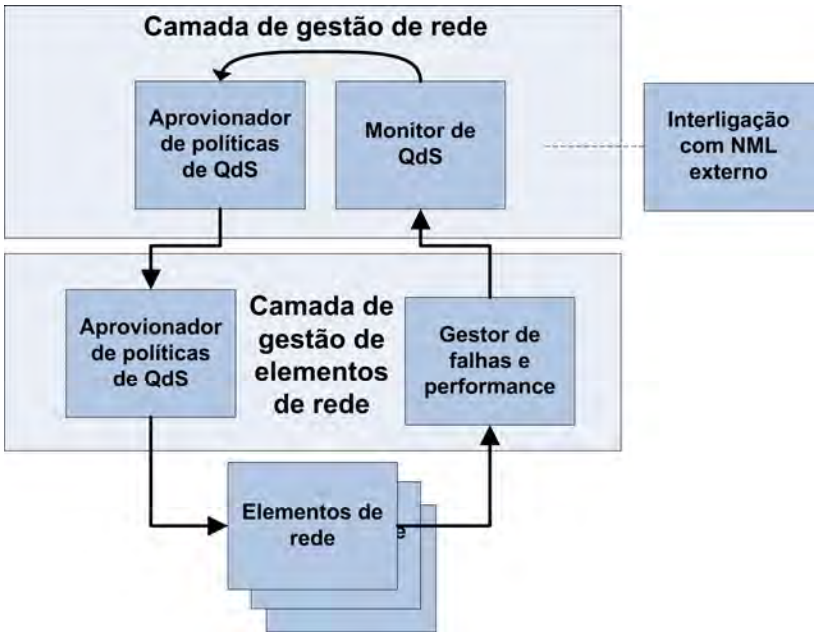

Figura 3.23 – Modelo de gestão de QdS proposto em [90].

Aprovisionamento de políticas de QdS

O aprovisionamento de políticas de QdS consiste na definição de regras que configurem e mantenham os NE para que eles implementem os serviços do cliente de acordo com o contracto negociado entre operador e o cliente. A monitorização de QdS consiste na recolha e análise dos

valores de QdS e respectivos alarmes, de forma a gerar relatórios acerca do desempenho do sistema. A informação desses relatórios é utilizada de forma efectuar alterações na configuração dos elementos de rede para que se cumpra o que foi contractualizado entre o operador e o cliente. As áreas funcionais são de seguida descritas.

O fornecimento de garantia de QdS entre extremos às aplicações dos clientes requer uma interacção entre as redes dos diferentes operadores. Adicionalmente existe uma grande diversidade de elementos de rede, de fabricantes e de fornecedores; com diferentes características, que devem ser configurados de uma forma consistente e à escala da rede do operador. A heterogeneidade dos elementos de rede a gerir implica a satisfação de um conjunto de requisitos que a solução de gestão de QdS deve cumprir: a automatização e centralização das tarefas de gestão, a configuração integrada dos elementos de rede à escala da rede do operador, o desenvolvimento de uma solução de configuração estável para as redes de grande dimensão, e que a solução seja baseada em soluções tecnológicas normalizadas de forma a poder inter operar com elementos de rede, bem como ao nível dos OSS.

A Figura 3.24 ilustra a arquitectura de aprovisionamento de políticas de QdS composta por 3 camadas, tal como o modelo geral de gestão definido na Figura 3.23.

O NML de aprovisionamento de políticas de QdS comunica com os aprovisionadores de políticas de QdS da camada de EML e com os PDP [92] através de uma interface do tipo *Itf-N* cuja especificação se encontra em mais detalhe nos documentos da série 32 do 3GPP.

Os aprovisionadores de políticas de QdS da camada EML, actuam como servidores de politicas ao nível da sua rede efectuando a distribuição de politicas pelas entidades PDPs da sua rede. Opcionalmente podem possuir uma interface de administração para o administrador da rede no caso da sua rede não possuir um aprovisionador de políticas de QdS da camada de rede, e possuem um repositório de politicas que armazena as politicas específicas da sua rede e todas as politicas comuns a todos os domínios. Os aprovisionadores de políticas de QdS da camada de gestão de rede fazem a distribuição integrada das políticas pelos PDPs do domínio e a detecção de conflito entre as politicas por si armazenadas.

Os aprovisionadores de políticas de QdS da camada EML estão interligados aos aprovisionadores da camada NML pela interface *Itf-N* e aos PDP pelas interfaces *Itf-Po*. As propostas em termos tecnológicos para a implementação das interfaces *Itf-Po* são LDAP, LDUP, SNMP e COPS-PR.

Na camada dos elementos de rede existem dois tipos de entidades lógicas: os PDPs e os PEP. Os PDPs decidem sobre as políticas a implementar e os PEPs implementam-nas nos elementos de rede. A interligação entre PDPs e PEPs é feita através da interface *Go* e que se

encontra especificada nos documentos TS 23.207 e TS 29.207 do 3GPP, e os protocolos propostos para a implementação desses interfaces são COPS-RSVP e COPS-PR.

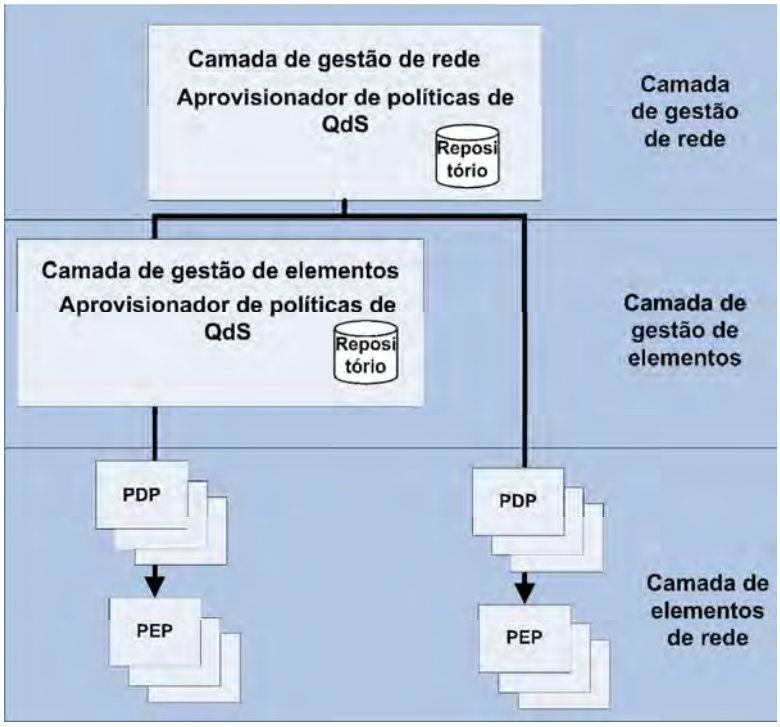

Figura 3.24 – Modelo de aprovisionamento de políticas de QdS proposto em [90].

As funções desempenhadas pelo PDP são: a recepção da informação relativa às políticas do servidor de políticas da camada EML, a análise da informação das políticas e a decisão de que acções deve executar, a distribuição dos dados das políticas pelos PEPs, a tradução das políticas do formato de politicas utilizado pelo servidor de políticas para o formato utilizado pelos PEPs, a tomada de decisões em tempo real quando inquirido pelos PEPS, e a detecção conflito de políticas em termos locais.

As funções desempenhadas pelos PEP são o armazenamento local dos dados relativas às políticas recebidas e a execução das configurações definidas nas políticas definidas pelo PDP.

Monitorização de QdS

A monitorização de QdS consiste na recolha e processamento de informação relativa à performance, à utilização e às faltas de QdS. A arquitectura de monitorização de QdS ilustrada na Figura 3.25 é uma arquitectura distribuída, também baseada em 3 camadas como a proposta de uma forma mais geral na arquitectura de gestão de QdS ilustrada na Figura 3.23.

O processo de monitorização de QdS pode ser sumariado pelas funções de: gestão das informações sobre falhas de QdS recebidas pelos elementos de rede, recepção dos dados de

performance de QdS recebidos dos elementos de rede, processamento dos dados recebidos, geração de relatórios de QdS com tendências da evolução dos parâmetros de QdS mais relevantes e análise dos dados de QdS obtidos comparativamente com os valores esperados.

Os elementos de rede da arquitectura são responsáveis pela recolha de medidas relativas à performance, pela recolha dos dados sobre a utilização dos recursos e pela geração de alarmes. Tal como no caso da arquitectura de aprovisionamento de politicas de QdS, os elementos de rede são distribuídos e constituídos por duas entidades funcionais: o PDP e PEP. As funções dos elementos de rede são: a recolha de informação de performance da rede de acordo com as definições das medidas e o seu envio para o servidor da camada EML; a recolha dos dados de utilização dos recursos e o seu envio para a camada de EML; e a detecção e recuperação de falhas, geração, eliminação, configuração e armazenamento de alarmes.

A entidade da camada de EML possui duas sub-entidades lógicas: o gestor de falhas e o gestor de performance. É responsável pela agregação e transferência dos dados relativos à performance, bem como dos eventos e alarmes gerados.

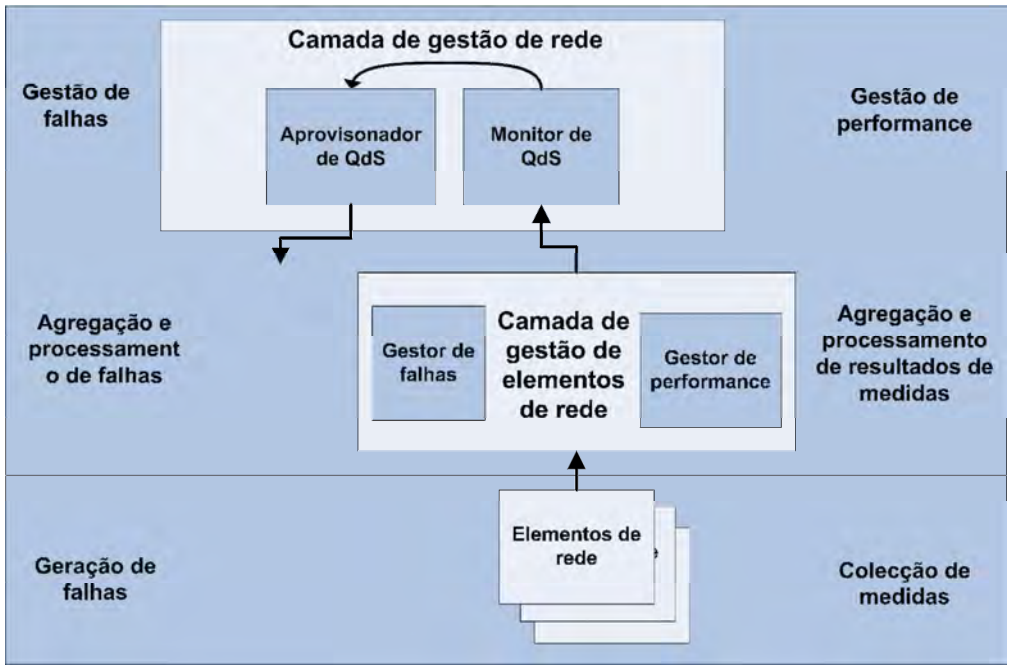

Figura 3.25 – Modelo de monitorização de QdS proposto do 3GPP [90].

O gestor de falhas executa a gestão de relatórios, de eventos e alarmes, o reencaminhamento em tempo real dos relatórios de alarmes, a recolha de informação dos NE a pedido do NM e o registo dos alarmes a pedido do NM. As funções executadas pelo gestor de performance incluem: a recolha dos dados de utilização dos recursos; a definição do formato de

especificação dos dados de medições, bem como da periodicidade dos relatórios; o envio dessa informação para o gestor da camada de NM ou armazenamento dos dados para a consulta pelo NM.

O gestor da camada NM é responsável por recolher e processar informação acerca de falhas, performance e utilização de recursos. Tem duas sub-entidades funcionais:

- ***Gestor de qualidade do serviço***: processa a informação de forma a determinar métricas de qualidade do serviço e interage com o gestor de politicas para desencadear acções correctivas quando estas forem consideradas necessárias. Esta sub-entidade recebe e processa a informação relativa à performance da rede e às falhas da mesma.
- ***O gestor de QdS do cliente***: recebe e processa a informação relativa à utilização de recursos e compara o serviço prestado aos utilizadores com os níveis de serviço definidos no contracto dos clientes.

3.3 Sumário

Nesta secção foi apresentada a arquitectura das redes de próxima geração, foram analisadas as propostas das principais organizações envolvidas na normalização das NGN e foram apresentadas as principais tecnologias de gestão de redes e de QdS por elas utilizadas.

As NGN consistem numa plataforma modular de gestão de elementos de rede e de serviços, capazes de fornecer serviços multimédia a utilizadores de uma rede de acesso heterogénea. Apesar das diferenças ao nível da nomenclatura, as propostas apresentam uma enorme semelhança em termos de arquitectura de rede, de separação entre a gestão do serviço e a gestão de rede, na utilização da plataforma IMS do 3GPP, bem como na utilização de políticas para a definição de critérios de admissibilidade de novas reservas.

A arquitectura de gestão das NGN proposta pelo 3GPP é uma arquitectura hierárquica composta por quatro camadas, onde a camada superior está relacionada com os sistemas de gestão empresarial. Apesar de ser ainda um trabalho em curso, a proposta define um conjunto de entidades e pontos de referência e propõe um conjunto de tecnologias de gestão para a implementação das interfaces. Para as camadas inferiores da tecnologia, propõem-se tecnologias de gestão eficientes essencialmente baseadas em protocolos binários com o SNMP e o COPS. No caso das camadas superiores da arquitectura as propostas incluem tecnologias de gestão baseadas em XML e em CORBA.

4 Arquitectura da plataforma de gestão

Neste capítulo propõe-se uma arquitectura para gestão de rede NGN. Começa-se por apresentar o conjunto de requisitos funcionais e não funcionais. É depois descrita a plataforma global de gestão, sendo apresentadas as funcionalidades dos elementos de cada uma das suas camadas, bem como o modelo de dados de gestão desenvolvido. Em seguida é descrita a solução que foi particularizada para a gestão de QdS, tanto ao nível do processo de configuração, como ao nível do comportamento dinâmico da plataforma.

4.1 Requisitos do sistema de gestão para redes NGN

O processo de levantamento de requisitos é uma componente fundamental da análise dos sistemas, pelo facto de evitar que alguns dos requisitos fundamentais do sistema a desenvolver sejam esquecidos durante o processo de desenvolvimento, bem como permitir que seja verificado o cumprimento de cada um dos requisitos identificados findo o desenvolvimento do mesmo.

A presente secção descreve o conjunto de requisitos que foram inicialmente definidos para o sistema de gestão, organizados em dois grupos: requisitos funcionais e não funcionais. Os requisitos funcionais definem condições a respeitar pelo sistema que o compõem. Os requisitos não funcionais representam condições que devem ser respeitadas pelo sistema de gestão, mas que não determinam características de um elemento do sistema em particular. Determinam tipicamente características de vários elementos do sistema, ou então do sistema de gestão como um todo.

Os requisitos funcionais (Tabela 4.1 e Tabela 4.2) descrevem um conjunto de condições que o comportamento dos elementos pertencentes ao sistema de gestão devem respeitar. No caso particular de uma rede NGN o levantamento de requisitos de gestão não é uma tarefa simples pois envolve operadores, utilizadores, empresas que operam na cadeia de valor da rede e muitos outros actores. Assim este trabalho teve em conta parte do trabalho desenvolvido pelo consórcio do 3GPP que efectuou um extenso levantamento, publicado em [90, 91, 93, 94].

Tabela 4.1 - Lista de requisitos funcionais gerais do sistema de gestão 3GPP TS 32.102.

REQ	DESCRIÇÃO	ÁREA	DOCUMENTO
Rf.1	Ser capaz de gerir equipamento de diferentes fabricantes.	Todo o sistema	3GPP TS 32.102
Rf.2	Desenvolver mecanismos de automatização de forma a optimizar eficiência e efectividade.		
Rf.3	Sistema de configuração deve ser suficientemente flexível de forma a que permita o rápido desenvolvimento de serviços.		
Rf.4	Deve reportar eventos e acontecimentos em formato normalizado de forma a permitir controlo remoto.		
Rf.5	Deve permitir interoperabilidade entre operador de rede e operadores de serviços para troca de informação de gestão e contabilização.		
Rf.6	Solução deve ser escalável e deve suportar redes de diferentes dimensões.		
Rf.7	Sistema de gestão deve permitir acesso a informação de gestão.		
Rf.8	Deve reutilizar normas das TI sempre que possível.		
Rf.9	Deve minimizar a complexidade de gestão da rede.		
Rf.10	Utilizar interfaces normalizadas para a comunicação entre os elementos de rede e elementos de gestão.		
Rf.11	Deve minimizar os custos de gestão.		
Rf.12	Fornecer um sistema integrado de gestão de falhas.		
Rf.13	Suportar operações de manutenção remotas de forma a simplificar interacções de suporte.		
Rf.14	Deve suportar gestão de segurança com ênfase particular em situações e roaming automático e em redes de troca de pacotes.		
Rf.15	Suportar mecanismos de facturação flexíveis de forma a se poderem aplicar entre redes de diferentes operadores.		
Rf.16	Suportar gestão e avaliação do desempenho.		
Rf.17	Centralizar informação para que a alteração de um parâmetro se repercuta em toda a rede à escala do domínio de gestão.		
Rf.18	Deve incluir mecanismos de restauração do sistema, (*e.g.*. re-sincronização e utilização de transacções).		

É ainda definido um conjunto de requisitos relacionados com áreas específicas, como a gestão de configuração, a gestão de falhas, o aprovisionamento de recursos ou a configuração de alarmes. Do mesmo modo, são definidos requisitos em relação às interfaces entre os elementos do cenário de gestão, bem como em relação aos protocolos de comunicação utilizados. A Tabela 4.2 enumera esses requisitos.

Tabela 4.2 - Lista de requisitos funcionais específicos de cada área de gestão.

REQ	DESCRIÇÃO	CUMPRIMENTO	ÁREA
Rf.19	Criação de recursos e elementos de rede.	Gestão de configuração	TS 132 600
Rf.20	Apagar recursos e elementos de rede.		
Rf.21	Configurar recursos e elementos de rede.		
Rf.22	Remover recursos da rede não operacionais, se necessário, de forma a minimizar distúrbios de funcionamento.		
Rf.23	Desacoplar modificações físicas das modificações lógicas.		
Rf.24	Completar todas as acções de configuração antes de disponibilizar recurso de rede.		
Rf.25	Interface de comunicação entre gestor central e elementos de gestão intermédia deve poder ser desligada.	Interface entre gestor central e gestores intermédios	
Rf.26	Informação deve poder ser enviada para o gestor central assim que produzida.		
Rf.27	Informação deve poder ser enviada para qualquer dos gestores centrais (um ou vários).		
Rf.28	Definição de limiares individuais para a geração de eventos.	Gestão de faltas Configuração de alarmes	TS 132.111
Rf.29	Capacidade de ser transportado em toda a rede independentemente da tecnologia de rede em questão (linhas dedicadas, X.25, ATM, Frame Relay, ...).	Protocolo de rede	3GPP TS 32.102
Rf.30	Representar um custo baixo e ser fiável.		
Rf.31	Detectar analisar e reportar eventos de falha de recursos.		
Rf.32	Efectuar a análise da localização das falhas.	Gestão de falhas de recursos	
Rf.33	Corrigir falhas de recursos.		
Rf.34	Sistema de reporte de falhas deve fornecer informação a outros processos de gestão de problemas.		
Rf.35	Sistema de administração de falhas deve gerir e verificar actividades de reparação de falhas.		
Rf.36	Verificar se recursos se encontram disponíveis.		
Rf.37	Reservar recursos necessários à disponibilização do serviços.	Aprovisionamento de recursos	
Rf.38	Efectuar reserva de recursos necessários para determinado período.		
Rf.39	Configurar e activar apropriadamente recursos.		
Rf.40	Testar e garantir que recurso funciona adequadamente e respeita valores de desempenho adequados.		
Rf.41	Actualizar inventário de recursos em repositório adequado.		
Rf.42	Deve permitir reconfigurar centralmente indicadores de severidade dos alarmes.		
Rf.43	Permitir a salvaguarda da informação de gestão.	Configuração de alarmes	TS 132.111

Os requisitos de facilidade de utilização identificam condições a respeitar pelo sistema de gestão, tipicamente relacionadas com a interacção com os actores humanos. Tendo em conta que o sistema de gestão segue o paradigma de gestão baseado em políticas, a interacção com os actores humanos concentra-se na interface gráfica de gestão. Dado que a solução de gestão aqui descrita se resume à gestão de recursos de rede, o único actor humano considerado é o administrador da rede. A Tabela 4.3 identifica os requisitos identificados, bem como a componente do sistema de gestão a que se aplicam.

Tabela 4.3 - Lista de requisitos da interface de utilizador.

REQ	DESCRIÇÃO	ÁREA
Rfu.1	Interface gráfica deve autenticar o administrador da rede junto ao CIMOM.	Interface gráfica
Rfu.2	Interface gráfica deve permitir acesso a todos os elementos de configuração do sistema.	Interface gráfica
Rfu.3	Interface gráfica deve permitir acesso a toda a informação de monitorização do sistema.	Sistema de gestão
Rfu.4	Interface de configuração deve permitir acesso a toda à lista de eventos do sistema.	Sistema de gestão
Rfu.5	Interface gráfica deve permitir a edição dos recursos da rede a gerir.	Interface gráfica
Rfu.6	Interface gráfica deve permitir ao administrador a visualização da lista de eventos.	Interface gráfica
Rfu.7	Interface gráfica deve permitir a edição dos serviços de rede.	Interface gráfica
Rfu.8	Interface gráfica deve permitir a edição dos serviços de A4C.	Interface gráfica
Rfu.9	Interface gráfica deve permitir a edição das políticas de forma gráfica, incluindo as três componentes da política: evento, condição e acção.	Interface gráfica
Rfu.10	Permitir a edição de políticas utilizando uma linguagem de especificação.	Interface gráfica
Rfu.11	Permitir a exportação de políticas para outros sistemas de gestão.	Interface gráfica
Rfu.12	Permitir a importação de outros sistemas de gestão.	Interface gráfica
Rfu.13	Proteger o sistema de erros cometidos pelo administrador do sistema no processo de especificação de políticas.	Interface gráfica
Rfu.14	Deve facilitar o processo de composição de políticas recorrendo a metáforas gráficas conhecidas.	Interface gráfica
Rfu.15	Deve auxiliar o administrador do sistema no processo de especificação de políticas minimizando dificuldades relativas ao conhecimento da sintaxe e da semântica das linguagens de especificação de políticas.	Interface gráfica

Os requisitos de desempenho (Tabela 4.4) estabelecem condições relativas ao desempenho dos vários elementos do sistema, tais como valores que reflectem as dimensões do cenário de gestão relativos ao tempo de resposta dos elementos do sistema às solicitações externas. Os requisitos de desempenho permitem definir, por exemplo, o número máximo de elementos de rede geridos pelo sistema e assim garantir que a solução desenvolvida apresente uma escalabilidade adequado.

Tabela 4.4 - Lista de requisitos de desempenho.

REQ	DESCRIÇÃO
Or.1	Sistema deve suportar rede com 40 milhões de utilizadores.
Or.2	Deve suportar a utilização de pelo menos 3 serviços em simultâneo por utilizador.
Or.3	Sistema deve efectuar a configuração de 20000 PCEF.
Or.4	Sistema deve efectuar a configuração de 10 PCRF.
Or.5	Sistema deve efectuar a configuração de 80000 interfaces de rede.

Seguindo a tendência apresentada nas várias arquitecturas NGN de reutilizar no desenvolvimento dos elementos, tanto quanto possível, soluções e tecnologias previamente normalizadas e interfaces abertas, é definido um conjunto de requisitos que traduzem essa tendência (Tabela 4.5).

Tabela 4.5 – Normas e regulamentação aplicáveis.

REQ	DESCRIÇÃO
NA.1	Utilização de soluções normalizadas.
NA.2	Utilização de interfaces abertas.
NA.3	Utilização de modelos de dados abertos, capazes de integrar a informação de gestão de toda a rede.
NA.4	Utilização de protocolos IEEE.
NA.5	Utilizar linguagens de especificação de políticas abertas e normalizadas.

São ainda definidos alguns requisitos para o sistema de gestão que derivam das melhores práticas do desenvolvimento de sistemas em geral e dos sistemas de software em particular. A Tabela 4.6 lista o conjunto desses requisitos.

Tabela 4.6 – Outros requisitos não funcionais.

REQ	DESCRIÇÃO
Or.1	Deve ser flexível, permitindo especificar novas políticas não previstas durante a análise de requisitos.
Or.2	Deve ser modular, permitindo instanciar novos elementos de gestão, aumentando assim a escalabilidade global.
Or.3	Deve ser autónoma permitindo a gestão dos equipamentos de acordo com as políticas definidas sem mais intervenção do operador humano.
Or.4	Deve ser robusta de forma a suportar falhas de comunicação entre elementos do cenário.
Or.5	Deve ser escalável permitindo gerir redes de operador de pequena, média ou grande dimensão.
Or.6	Deve recuperar a falhas, especialmente a falhas de comunicação entre elementos do sistema de gestão.
Or.7	Deve poder ser facilmente integrada com sistemas empresariais do operador de forma permitir a integração entre sistemas de gestão da rede e gestão do negócio.

Foi planeada e desenvolvida uma solução de gestão que se descreve na seguinte secção, e que cumpre esses requisitos.

4.2 Descrição global da solução de gestão

A arquitectura proposta assenta no modelo de gestão distribuída baseada no paradigma de gestão PBM. É constituída por 3 camadas seguindo o modelo de gestão proposto pelo 3GPP [90] e descrito em 3.2.2:

- a camada de gestão de rede é composta pelo gestor de rede, pelo repositório central de informação de gestão e pela lógica de adaptação à camada de gestão dos elementos;
- a camada de gestão dos elementos é composta por um conjunto de gestores de nível intermédio, responsáveis pela gestão de aspectos específicos de cada área de gestão;
- a camada de elementos de rede é constituída por sistemas responsáveis por pôr em prática as acções de configuração, determinadas pelos elementos da camada de gestão dos elementos.

A Figura 4.1 ilustra a arquitectura proposta.

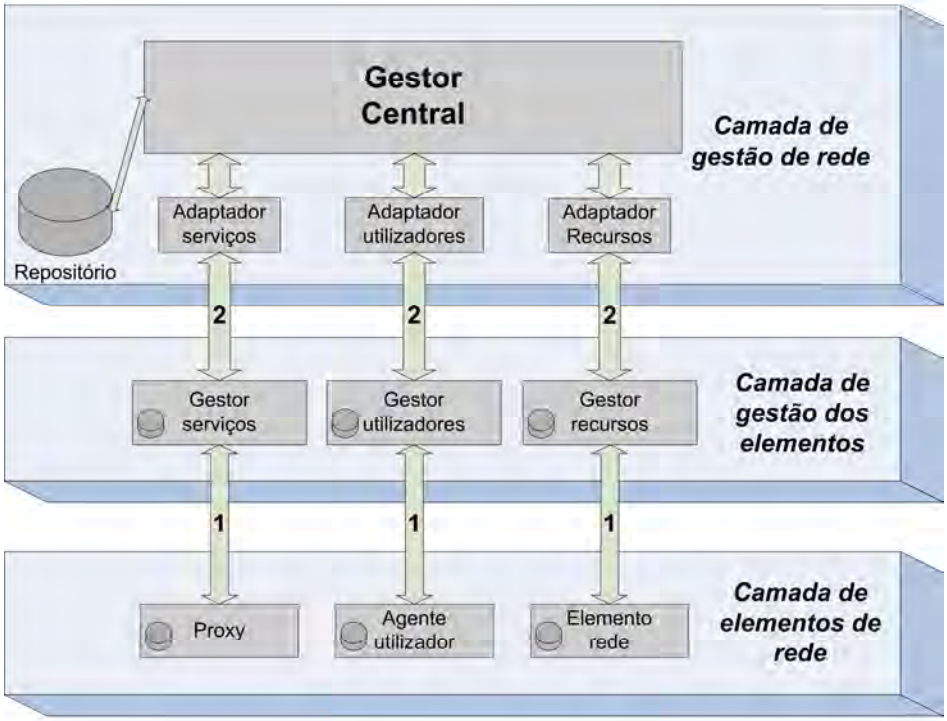

Figura 4.1 – Arquitectura geral da solução de gestão.

A utilização de um servidor central de gestão permite criar um ponto único de contacto com o administrador do sistema, permitindo a configuração de todos os elementos à escala do domínio de gestão, bem como consultar toda a informação relevante acerca do funcionamento dos elementos da rede. Essa interacção pode ser efectuada através de uma aplicação gráfica, descrita na secção 4.3. O servidor central de gestão encarrega-se de distribuir a informação de configuração pelos elementos da camada intermédia, fazendo a adaptação da informação ao formato específico de cada elemento de gestão intermédio. Por exemplo, a definição de uma determinada regra pode envolver acções relacionadas com a gestão de utilizadores, gestão de recursos e a gestão de serviços. É para isso necessário que o gestor central entregue cada componente dessa regra ao elemento adaptador adequado ao aspecto em questão e que o adaptador se encarregue de efectuar a distribuição dessa informação por todos os elementos da camada inferior (*e.g.*: todos os gestores de recursos) à escala da rede do operador.

Este processo de adaptação da informação de gestão, tradicionalmente referido por refinamento de políticas, é necessário uma vez que as diferentes entidades da camada inferior podem dialogar utilizando diferentes protocolos. A adaptação da informação é feita pelos

elementos adaptadores, seguindo um princípio de funcionamento semelhante ao utilizado por Neisse em [95].

Pertencem à camada intermédia os elementos gestores de áreas específicas da gestão. Existem elementos gestores de recursos, que se responsabilizam por efectuar controlo de admissão, bem como por definir a quantidade de recursos atribuídos a cada reserva; existem elementos gestores de utilizadores, que se encarregam da gestão de utilizadores e seus perfis (*e.g.:* autenticação, autorização, contabilização); e existem elementos gestores dos serviços que se encarregam de gerir todos os aspectos relacionados com os serviços, como definir *codecs* e protocolos de transporte a utilizar. A quantidade de elementos gestores intermédios de cada tipo pode ser alterada de forma manter a escalabilidade do sistema.

Na camada dos elementos de rede existe um conjunto de elementos actuadores que põe em prática as configurações recebidas pelos elementos da camada de gestão intermédia. Podem apontar-se como exemplos de elementos desta camada encaminhadores da rede, agentes de utilizadores, *proxies* de serviços ou ainda servidores de conteúdos. Recebem instruções de configuração dos elementos da camada superior e contactam-nos pedindo informações ou exportando decisões num processo semelhante ao implementado nos sistemas baseados no paradigma de COPS-RSVP.

O carácter distribuído da solução de gestão permite-lhe preservar a escalabilidade, visto que os elementos de gestão intermédia são especializados na sua área de gestão específica e que sendo possível replicar cada um destes elementos se consegue distribuir a carga computacional. É ainda uma solução flexível visto que é possível ao gestor central impor todas as acções de configuração que sejam suportadas pelos elementos das camadas inferiores.

A subsecção que se segue apresenta uma descrição da componente de gestão de QdS, vertente em que se centrou este trabalho.

4.2.1 Arquitectura do gestor de QdS

Por questões de simplicidade, o presente trabalho centra-se na componente da arquitectura responsável pela gestão de QdS. O sistema de gestão de QdS, ilustrado na Figura 4.2, segue a arquitectura descrita na secção 4.2 mantendo as três camadas: a primeira camada possui um gestor global com a necessária lógica de adaptação; a segunda possui com conjunto de elementos gestores de recursos de rede; e a terceira um conjunto de elementos de rede que implementam as decisões da camada anterior.

O gestor global do sistema é baseado na tecnologia WBEM, desenvolvido com base num servidor de gestão em código aberto OpenWBEM [23]. Tal opção deveu-se a vários factores:

- ao facto de existirem várias implementações de código aberto baseadas na tecnologia WBEM que permitem um desenvolvimento rápido da solução de gestão;
- à existência de uma vasta comunidade de desenvolvimento que oferece suporte e que permite reutilizar uma aplicação depurada de erros de desenvolvimento;
- à flexibilidade apresentada pelo modelo de dados da tecnologia que permite integrar a gestão de recursos da rede, a gestão dos serviços prestados com as políticas que gerem os sistemas;
- ao facto de o modelo de dados CIM ser orientado a objectos e facilmente extensível;
- à interoperabilidade oferecida pelas tecnologias baseadas na Web como XML e HTTP.

A camada de gestão desta arquitectura possui um repositório interno e contém três adaptadores que implementam a comunicação com os elementos da camada inferior:

- ***Adaptador de configuração***: implementa a configuração dos elementos da camada intermédia, adaptando a informação de configuração existente no servidor central a cada um dos elementos da camada intermédia e efectuando a transmissão dessa informação;
- ***Adaptador de eventos***: funciona como colector que processa, reformata e entrega eventos ao gestor de eventos do CIMOM;
- ***Adaptador de políticas***: funciona como um executor de políticas do CIMOM. Subscreve eventos e, ao ser notificado da ocorrência de um evento, analisa as regras que devem ser despoletadas por esse evento. Se as condições pertencentes à regra forem verdadeiras o adaptador invoca os métodos correspondentes às acções definidas na regra.

A comunicação entre o elemento de gestão central e os elementos da camada intermédia é feita através de uma interface implementada pelos adaptadores. Funciona como um *gateway* de sinalização entre o protocolo de comunicação utilizado pela tecnologia WBEM e o protocolo de comunicação utilizado na comunicação com o elemento da camada intermédia. A adaptação da informação de gestão é efectuada recorrendo a duas tecnologias: NETCONF para a transferência de informação de configuração e de eventos e Diameter para a transferência da informação de políticas. O protocolo NETCONF foi normalizado pelo IETF e têm vindo a ser propostas aplicações do protocolo para as áreas de configuração de equipamentos de redes [96, 97] e de monitorização de eventos [98]. O protocolo Diameter tem vindo sucessivamente a ser proposto pelo 3GPP como protocolo a utilizar nas interfaces de comunicação das entidades da plataforma IMS. A escolha do protocolo Diameter para efectuar a transferência de políticas entre o gestor central e os elementos gestores intermédios deveu-se ao facto de esse protocolo ter sido utilizado pelo 3GPP para a implementação da interface *Gx* na plataforma PCC [52] efectuando a

comunicação de informação de políticas entre os elementos de gestão intermédios e os elementos de rede.

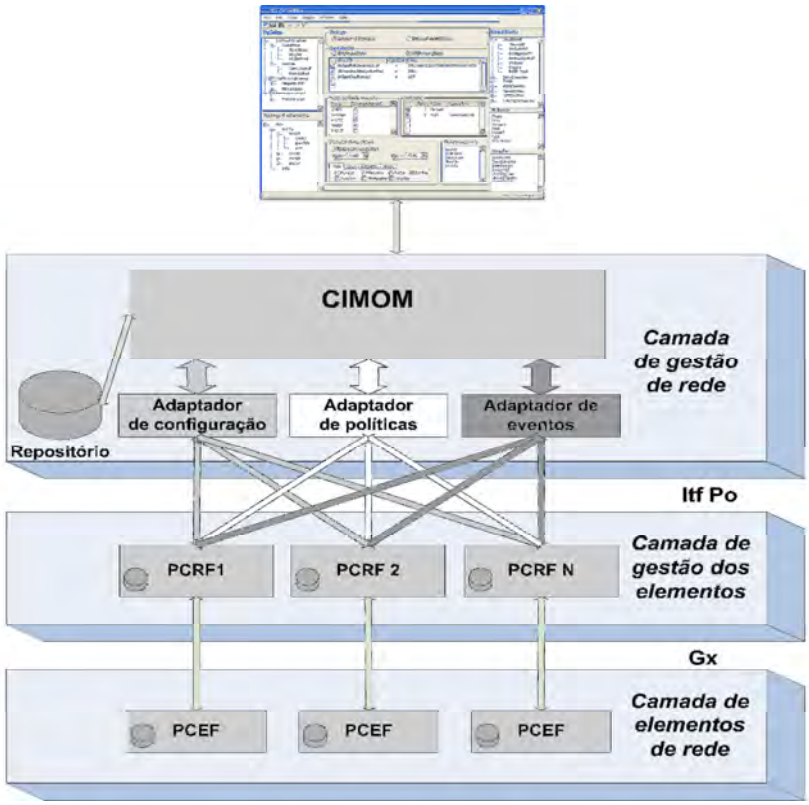

Figura 4.2 - Arquitectura de gestão de QdS.

Cada um dos adaptadores estabelece ligações com vários elementos da camada inferior, que são responsáveis pela gestão dos elementos de rede. Os gestores de recursos efectuam controlo de admissão de novos fluxos de pacotes e fazem reconfiguração dos elementos de rede de forma a manterem prioritização do tráfego de acordo com os requisitos de QdS de cada um dos serviços. São responsáveis por uma quantidade de elementos da camada inferior, com os quais estabelecem comunicação, efectuam a configuração, recebem pedidos de decisões e dos quais recebem informação da ocorrência de eventos. A definição do conjunto de elementos da camada inferior que é configurada por cada elemento da camada intermédia segue um critério de proximidade geográfica. A granularidade da divisão tem a ver com a quantidade de acções de configuração requeridas pela rede.

Os elementos da camada inferior são encaminhadores da rede que conduzem os pacotes de cada um dos serviços. Recebem configurações do seu gestor da camada intermédia e, mediante requisitos dos serviços, solicitam que determinadas decisões sejam tomadas.

4.2.2 Modelo de dados do gestor

A informação de gestão do sistema é armazenada no repositório utilizando um conjunto de classes definidas como extensões ao modelo CIM. Estas extensões encontram-se representadas, de acordo com a sua funcionalidade, segundo quatro sub-modelos: modelo de recursos, modelo de serviços, modelo de eventos e modelo de políticas.

O modelo de recursos, que se encontra ilustrado na Figura 4.3, contém um conjunto de classes que representam os elementos de rede.

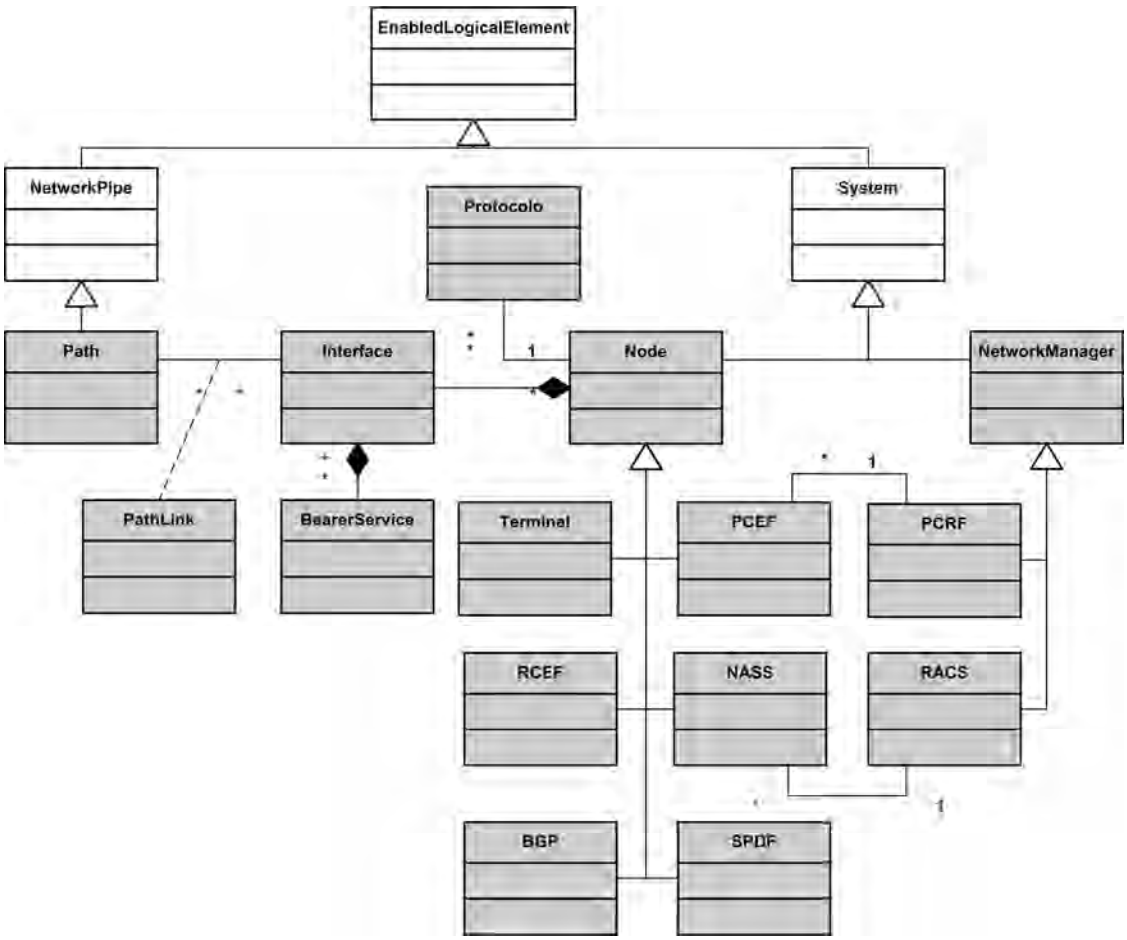

Figura 4.3 - Modelo de recursos de rede.

Em todos os diagramas de classes UML apresentados nas figuras seguintes, as classes pertencentes ao modelo CIM encontram-se representadas a branco, enquanto que as extensões propostas se encontram representadas a cinzento. Os elementos de rede são modelados como extensões da classe *System.* Dessa classe são derivadas duas classes abstractas: a classe *Node* que representa o nó de rede, como um terminal ou um *router*; e a classe *NetworkManager*, que representa elementos gestores de recursos de rede. Da classe *NetworkManager* derivam dois tipos de gestores: o PCRF representando o gestor de recursos da rede 3GPP e o RACS representando o

gestor de recursos de rede relativa à rede TISPAN. Os elementos derivados da classe *Node* representam elementos de encaminhamento de tráfego, quer da rede TISPAN, quer da rede 3GPP, bem como os terminais que representam os terminais utilizados pelos clientes da rede.

Os nós da rede são constituídos por interfaces, representados pela classe *Interface* que possuem a possibilidade de barrar a condução de um fluxo, representado pela classe *BearerService*. Também participam no caminho percorrido pelos fluxos de pacotes, aqui representados pela classe *Path*. A classe *Path* foi derivada da classe do modelo CIM designada de *NetworkPipe*, representando percursos que o tráfego pode percorrer no interior da rede.

Os serviços disponibilizados pela rede requerem que sejam reservados alguns dos recursos existentes para que os pacotes sejam transportados. A Figura 4.4 ilustra o modelo de serviços proposto, descrevendo as classes utilizadas para representar a informação relativa aos serviços.

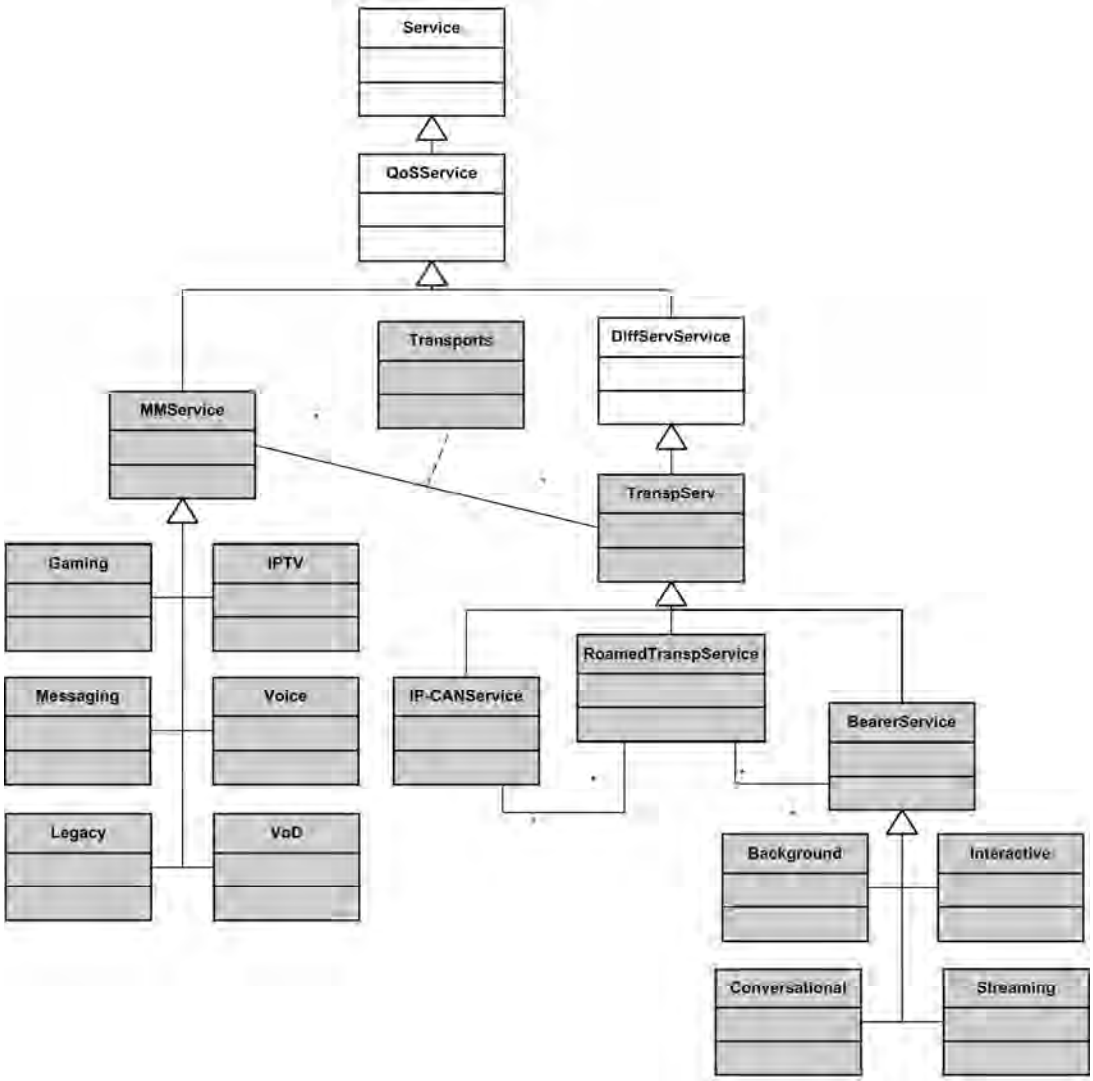

Figura 4.4 - Modelo de serviços.

Sendo um requisito da generalidade das redes NGN que seja uma rede IPv6 com mecanismos de QdS baseados em *Diffserv,* todos os serviços foram representados através de uma derivação da classe abstracta do modelo CIM *DiffServ*. Foram derivadas duas classes abstractas *MMService* e *TranspServ*: a classe *MMService*, representa serviços multimédia que são representados através de classes derivadas de *MMService* como por exemplo *Gaming*, *Messaging*, *IPTV*, *Voice*, *VoD* e *Legacy*; e a classe *TranspServ* representa os serviços de transporte *BearerService*, *RoamedTranspService* e *IP-CANService*. A classe *BearerService* é ainda estendida para representar os serviços definidos pelo consórcio 3GPP nas classes *Background*, *Interactive*, *Conversational* e *Streaming*.

A classe *RoamedTranspService* representa serviços de rede prestados a utilizadores fora da sua rede que são mapeados pelo operador como um serviço equivalente ao serviço contractualizado pelos utilizadores na sua rede original.

O modelo de eventos, ilustrado na Figura 4.5, representa um conjunto de classes que foram derivadas do modelo de eventos do CIM [30].

Na base do modelo de eventos existe uma classe *Indication* que representa, tal como no modelo de eventos CIM, um evento de interesse para o sistema de gestão. Os eventos podem ser do tipo *InstanceIndication* que modela alterações, criações ou eventos de remoção de instâncias, ou alertas representados pela classe abstracta *AlertIndication*. Os alertas podem ainda estar relacionados com uma grandeza e com limiares definidos para a sua variação e são aqui representados pela classe *ThresholdIndication.* Podem também estar relacionados com a ocorrência de um acontecimento, modelado em CIM através da classe abstracta *AlertInstIndication*.

Foram identificados vários exemplos de eventos com interesse para a gestão do sistema e foram desenvolvidas extensões às classes CIM, representadas a cinzento no diagrama da Figura 4.5.

Segundo o modelo CIM as entidades de gestão devem subscrever a recepção dos eventos para que o gestor, tipicamente implementado pelo CIMOM, as notifique sempre que o evento em questão ocorrer. A subscrição, implementada pela classe de associação *IndicationSubscription,* define o elemento de gestão subscritor das indicações que é modelado pela classe *ListenerDestination;* bem como um filtro que define quais os eventos de que a entidade subscritora pretende ser notificada e que é modelado através da classe *IndicationFilter*.

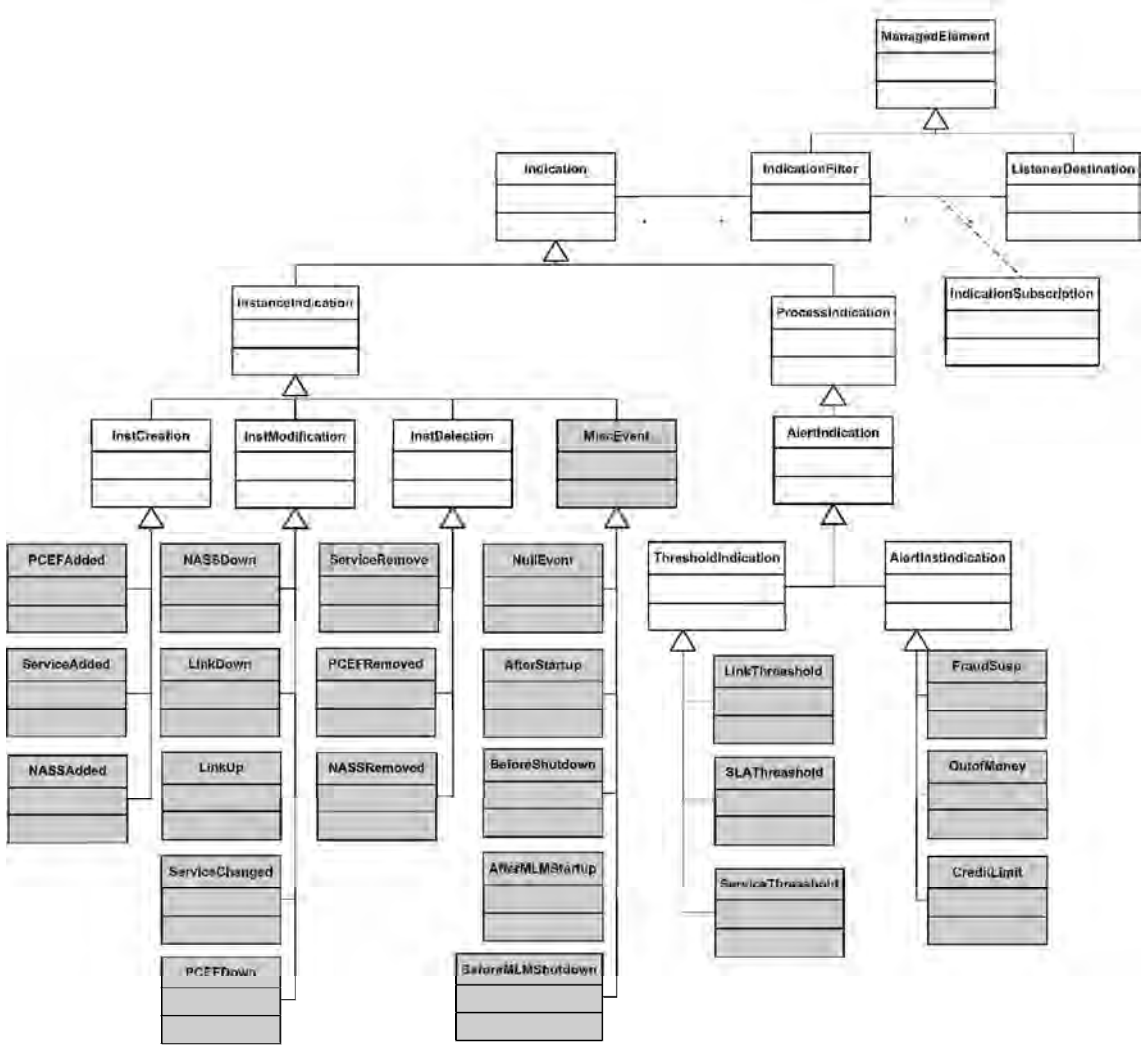

Figura 4.5 – Modelo de eventos.

O modelo de políticas proposto encontra-se esquematizado, de forma resumida, na Figura 4.6. Uma versão mais completa é apresentada no Anexo C.

O modelo proposto segue o modelo de políticas CIM, acrescentando-lhe algumas extensões, que a seguir se descrevem resumidamente. As políticas em CIM são representadas através da classe abstracta *PolicySet* que permite a aglomeração de políticas. Da classe *PolicySet* são estendidas as classes *PolicyRule* que efectivamente representa a política e a classe *PolicyGroup* representando um grupo de políticas. São elementos de uma regra uma ou mais condições, modelados através da classe *PolicyCondition,* e um conjunto de acções ou grupos de acções modelado pela classe *PolicyAction*.

Segundo o modelo CIM não existe qualquer relação entre o modelo de políticas e o modelo de eventos, sendo impossível representar políticas passíveis de ser despoletadas por um evento externo. Na ausência de um evento que consiga despoletar a avaliação de políticas, o servidor de

gestão tem duas alternativas: ou avalia as políticas durante o arranque do sistema e executa-as no caso as suas condições sejam verdadeiras; ou então o servidor de gestão permanece continuamente a verificar a veracidade das condições das diversas políticas do sistema, de forma a decidir quando as executar. A primeira hipótese é muito limitadora relativamente ao tipo de políticas que se podem definir, a segunda torna o sistema consideravelmente consumidor de recursos computacionais pelo facto de as condições serem avaliadas continuamente.

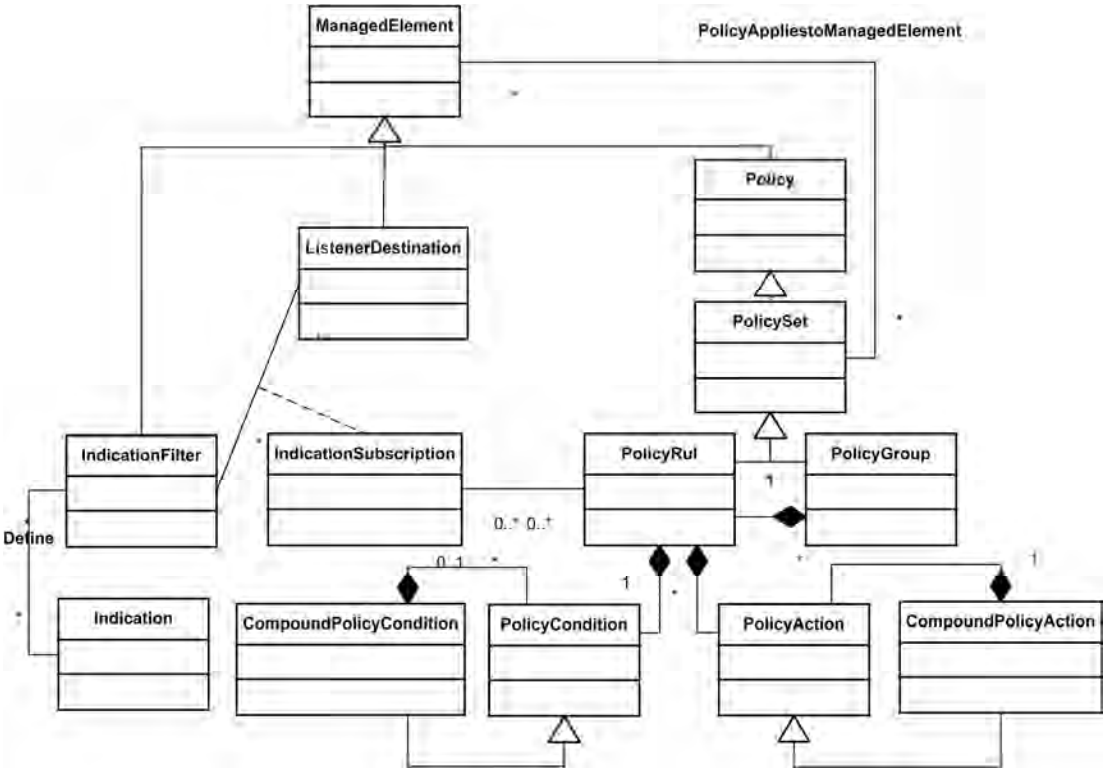

Figura 4.6 - Modelo de políticas.

O modelo de dados proposto resolve a falta de dinamismo das políticas em CIM através da criação de uma relação entre a classe *CIM_PolicyRule* e a classe associação *CIM_IndicationSubscription*, dotando a política de uma componente dinâmica capaz de despoletar a sua execução. Durante o processo de especificação de políticas, descrito em 4.4.2, é efectuada a subscrição dos eventos que devem despoletar a política. A componente do gestor encarregue da execução de políticas (neste caso o adaptador de políticas) subscreve essas indicações. Quando a indicação lhe é enviada o adaptador de políticas verifica quais as políticas que incluem essa subscrição, verifica as suas condições e, quando as condições são verdadeiras, executa as suas acções.

4.2.3 Adaptadores de gestão

O CIMOM é um gestor de objectos CIM genérico que pode ser aplicado a qualquer contexto de gestão. Existem aplicações de gestão desenvolvidas com base na tecnologia WBEM para áreas tão diversas como gestão de equipamentos de redes, gestão de servidores de correio electrónico ou gestores de servidores de armazenamento de dados. Da mesma forma, o modelo de dados CIM é um modelo orientado a objectos genéricos, que pode representar informação de qualquer domínio de gestão. Para ser aplicado a cenários de gestão concretos, pressupõe a criação de extensões específicas capazes de representar as especificidades dos elementos geridos de cada cenário. A criação de novas classes, com novos atributos e novos métodos, faz com que o gestor genérico de objectos CIM sozinho não consiga gerir os objectos resultantes das extensões.

Segundo a arquitectura típica das soluções de gestão WBEM, a adaptação do motor genérico CIM às especificidades dos objectos é feita através da criação de adaptadores, designados na literatura como *providers*. Estes são implementados como componentes dinâmicas e são carregados pelo CIMOM sempre que este necessita de manipular um objecto de uma classe pertencente ao *Extensions Schemas* do CIM.

Os adaptadores de configuração e de eventos utilizam uma interface de comunicação baseada em NETCONF, fazendo a adaptação das mensagens WBEM para NETCONF, bem como a adaptação inversa. A forma como as mensagens são traduzidas entre tecnologias encontra-se descrita na Tabela 4.7.

Tabela 4.7 - Adaptação de mensagens entre tecnologia WBEM e NETCONF.

PROPÓSITO	WBEM	NETCONF	DIAMETER
Leitura de valor de uma instância.	GetInstance	<get-config>/<get>	Policy-Data-Request
Enumeração de instâncias	EnumerateInstances	<get-config>	Policy-Data-Request
Criação de instância	CreateInstance	<edit-config>	Policy-Install-Request
Modificação de instância	ModifyInstance	<edit-config>	Policy-Install-Request
Apagar instância.	DeleteInstance	<delete-config>	Policy-Install-Request
Envio de indicação	ExportIndication	<notification>	
Invocação de método	InvokeMethod		Policy-Install-Request

No caso do adaptador de políticas a comunicação com os elementos gestores intermédios é feita através da utilização de uma interface Diameter. Esta efectua a tradução de mensagens entre as tecnologias WBEM e Diameter, de acordo com a equivalência descrita na Tabela 4.7. Além de ser implementado como um adaptador WBEM, o adaptador de políticas é simultaneamente um consumidor de eventos. Para isso, no seu processo de arranque, regista-se subscrevendo a recepção das indicações que pretende receber. Quando as recebe verifica quais as políticas relacionadas com a indicação recebida e executa-a.

A utilização de duas tecnologias diferentes para a adaptação de informação de gestão foi feita de forma a utilizar as melhores características de cada uma delas. Por um lado a tecnologia NETCONF tem vindo a ser normalizada e promovida pelo do IETF como sucessora das tecnologias SNMP e COPS e fornece suporte de configuração e notificação de eventos, tendo fortes possibilidades de se afirmar como tecnologia de futuro. Por outro lado a tecnologia Diameter foi utilizada pelo 3GPP na arquitectura da plataforma de PCC no desenvolvimento da interface Gx, transportando informação de políticas entre o PCRF e o PCEF. A utilização da tecnologia Diameter pelo adaptador de políticas evita que o elemento gestor intermédio tenha que efectuar recodificação das políticas quando as distribui para os elementos de rede.

4.3 Configurador do sistema de gestão

O modelo proposto para a interacção com o administrador do sistema tem um ponto de contacto unificado, implementado através de uma aplicação gráfica que efectua a edição de todos os dados relativos à gestão de todos os equipamentos.

A subsecção actual descreve a proposta de uma aplicação gráfica, projectada para simplificar a tarefa do administrador do sistema: reduzindo a complexidade da tarefa de especificação dos dados de gestão; evitando a necessidade de conhecer detalhadamente os pormenores do cenário de gestão; e representando isoladamente a sintaxe dos *scripts* de configuração. A aplicação permite definir políticas de uma forma gráfica bem como através de uma interface de texto, que permite a especificação de regras na linguagem CIM-SPL.

4.3.1 Editor de políticas

A componente de edição gráfica de políticas pode ser utilizada de duas formas:

1. efectuar a criação de regras ou grupos de regras através da utilização de um assistente;
2. compor graficamente cada aspecto da regra numa interface gráfica onde lhe são disponibilizados todos os elementos da regra, bem como todos os elementos passíveis de serem utilizados na sua composição.

A Figura 4.7 ilustra alguns dos passos do assistente de criação de uma nova política. Cada uma das janelas contém um conjunto de elementos, agrupados de acordo com as diversas componentes de uma política CIM, que devem ser preenchidos pelo administrador de forma a especificarem os pormenores da regra.

O assistente de criação de grupos de políticas é mais simples do que o assistente de criação de regras; tem menos janelas e limita-se a pedir ao administrador do sistema que seja definido o nome do grupo criado e que seja identificado o grupo pai.

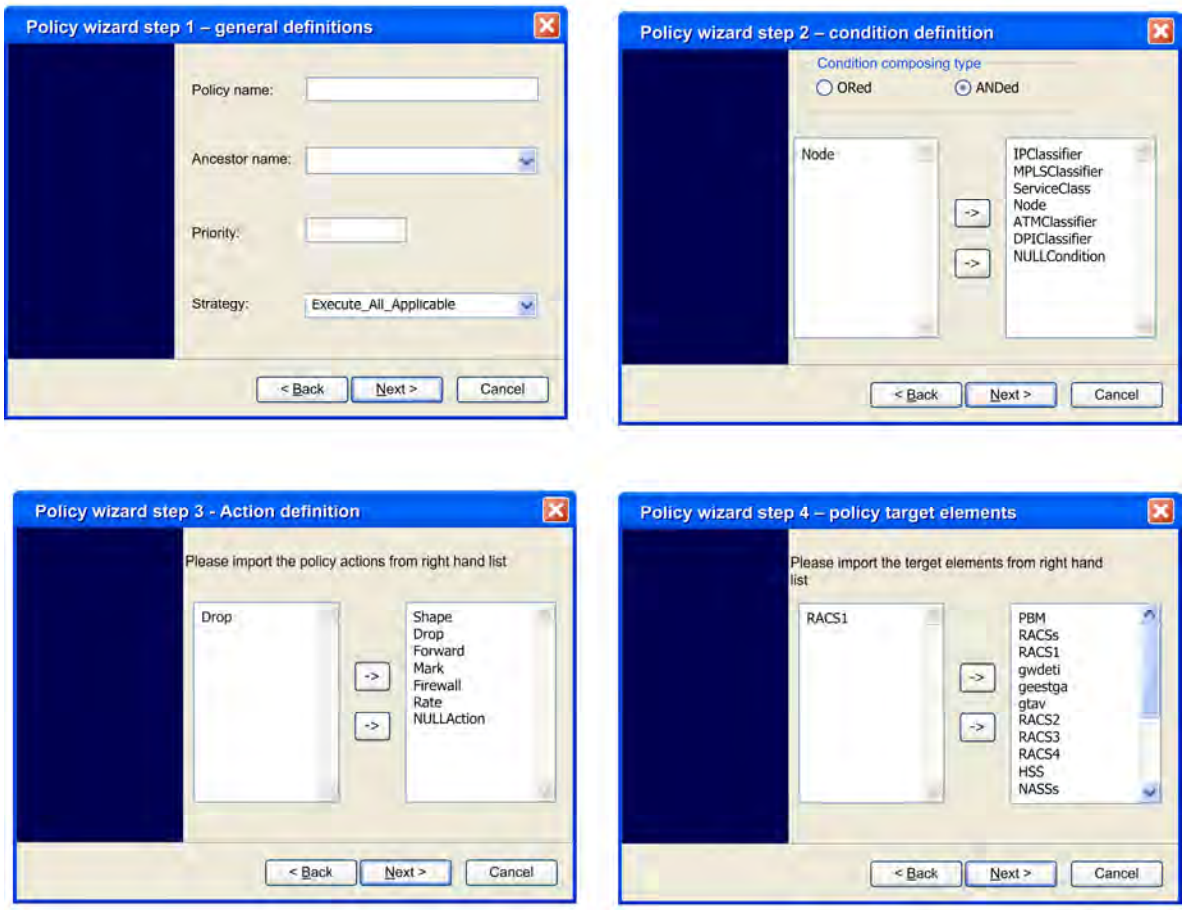

Figura 4.7 - Assistente de criação de políticas.

Findo o processo de especificação da política, a aplicação gráfica efectua a inserção no CIMOM da informação relativa às diversas componentes da mesma. A aplicação permite ainda que a informação da política seja posteriormente editada através da interface gráfica ilustrada na Figura 4.8.

A interface de composição gráfica das regras, ilustrada na Figura 4.8, consiste numa aplicação gráfica que descreve cada um dos componentes pertencentes à política na área central da janela. São aí definidos os pormenores relativos à estratégia de execução da política: as condições e as acções constantes da política, o período de tempo no qual é válida, os elementos sobre os quais a política se aplica, bem como a lista de eventos capazes de a despoletar.

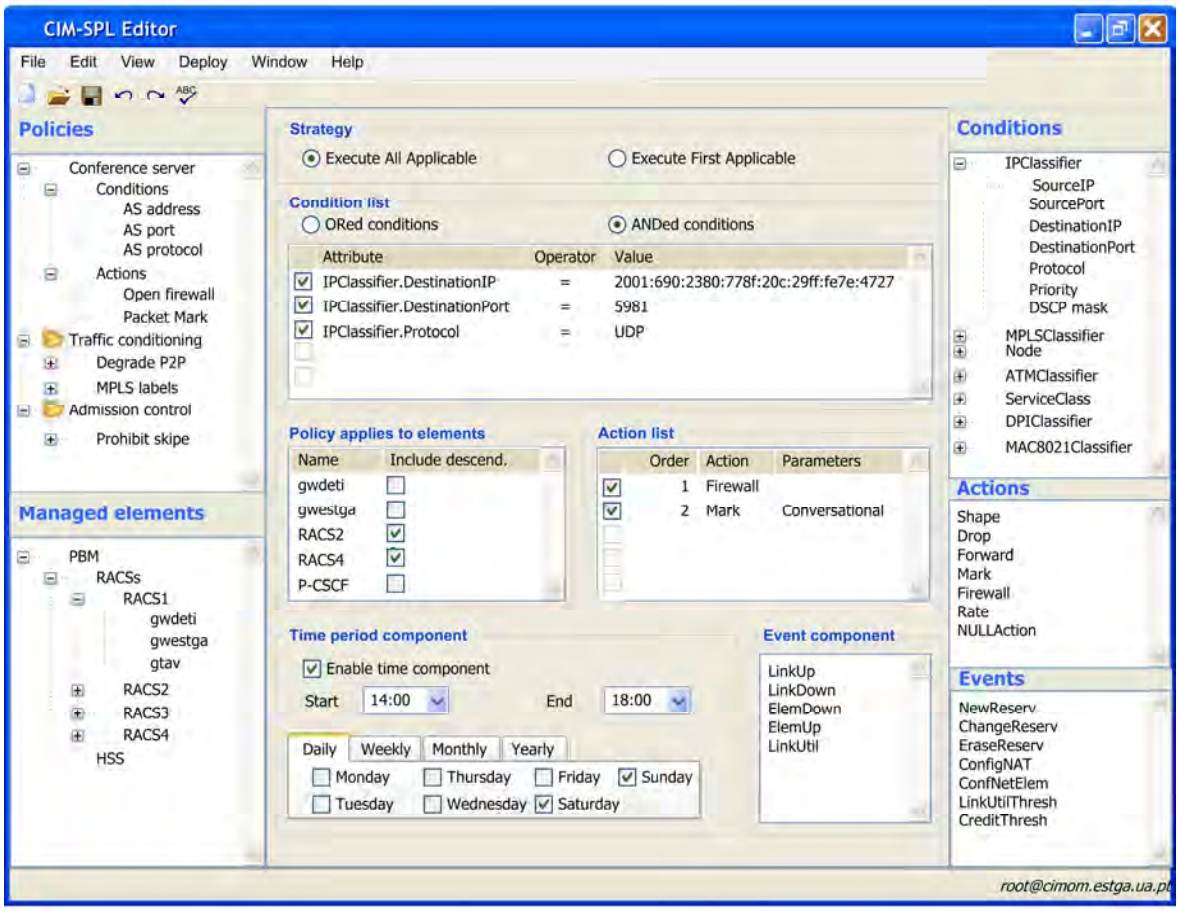

Figura 4.8 - Editor gráfico de políticas.

Nas áreas periféricas são representados os elementos susceptíveis de serem utilizados na especificação dos vários componentes da política: listam-se de forma hierárquica os grupos e políticas existentes no sistema (*Policies*), enumeram-se os elementos pertencentes ao cenário de gestão (*Managed Elements*), listam-se as condições passíveis de ser verificadas pela plataforma de gestão (*Condition*), é fornecida uma lista de acções que o sistema de gestão pode implementar (*Action*) e é definida a lista de eventos que podem ser utilizados para despoletar a execução de políticas (*Events*). A utilização dos elementos fornecidos para a composição de políticas é feita através de acções de arrastamento dos elementos para a área da janela onde se encontra a componente da política relacionada.

A interface é constituída por elementos gráficos comuns à maioria das aplicações actuais, permitindo assim uma adaptação fácil do administrador à aplicação de gestão [99].

4.3.2 Browser de políticas

A aplicação gráfica dispõe ainda de um browser de políticas com o objectivo de facilitar a procura e activação das regras presentes no servidor. É constituída por uma lista hierárquica de políticas e grupos onde é possível efectuar o arrastamento dos componentes de um local da árvore para outro, originando assim uma alteração do grupo pai.

A interface permite a activação ou desactivação de uma política através do botão existente na primeira coluna, bem como a edição de uma das políticas através de um clique duplo em cima da linha onde se encontra listada, utilizando para isso a componente do editor ilustrada na Figura 4.8.

A facilidade de pesquisa de políticas permite procurar as regras existentes de acordo com critérios como: o nome da política, o grupo a que pertence ou os elementos de rede a que se aplica. Esta facilidade permite mais facilmente procurar e activar regras em cenários de gestão reais onde o número de políticas residentes na plataforma de gestão pode tornar morosa e difícil a procura de uma regra entre todas as outras.

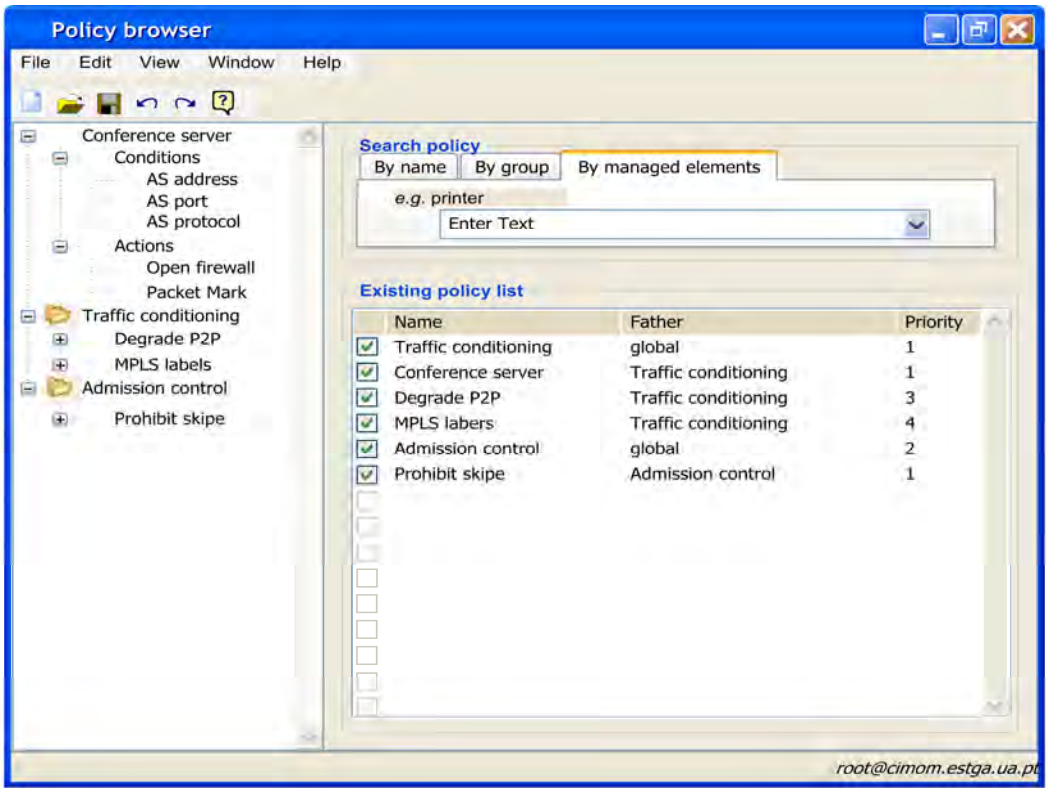

Figura 4.9 - Browser de políticas.

As ferramentas gráficas de edição de políticas descritas na actual subsecção permitem uma atenuação da curva de aprendizagem do processo de especificação de políticas. A utilização de

assistentes para a especificação de políticas permite a correcta definição da regra em todas as suas componentes, mesmo por parte de um utilizador que não conheça todos os seus componentes.

4.3.3 Editor de CIM-SPL

A interface gráfica inclui ainda um editor de CIM-SPL, como ilustrado em Figura 4.10, de forma a permitir a utilizadores mais experientes efectuar a especificação de políticas textualmente.

O editor de CIM-SPL consiste num editor de texto integrado na aplicação gráfica que permite a edição de políticas utilizando a linguagem SPL. Inclui funcionalidades de cópia e colagem de texto e de serialização das políticas de e para ficheiros de texto. Permite a exportação e importação de políticas em formato SPL e assim efectuar a salvaguarda de políticas definidas, bem como a transferência de políticas entre diferentes servidores. Permite ainda a utilização de *scripts* de forma a efectuar a replicação de políticas em situações em que estas difiram de pequenos pormenores.

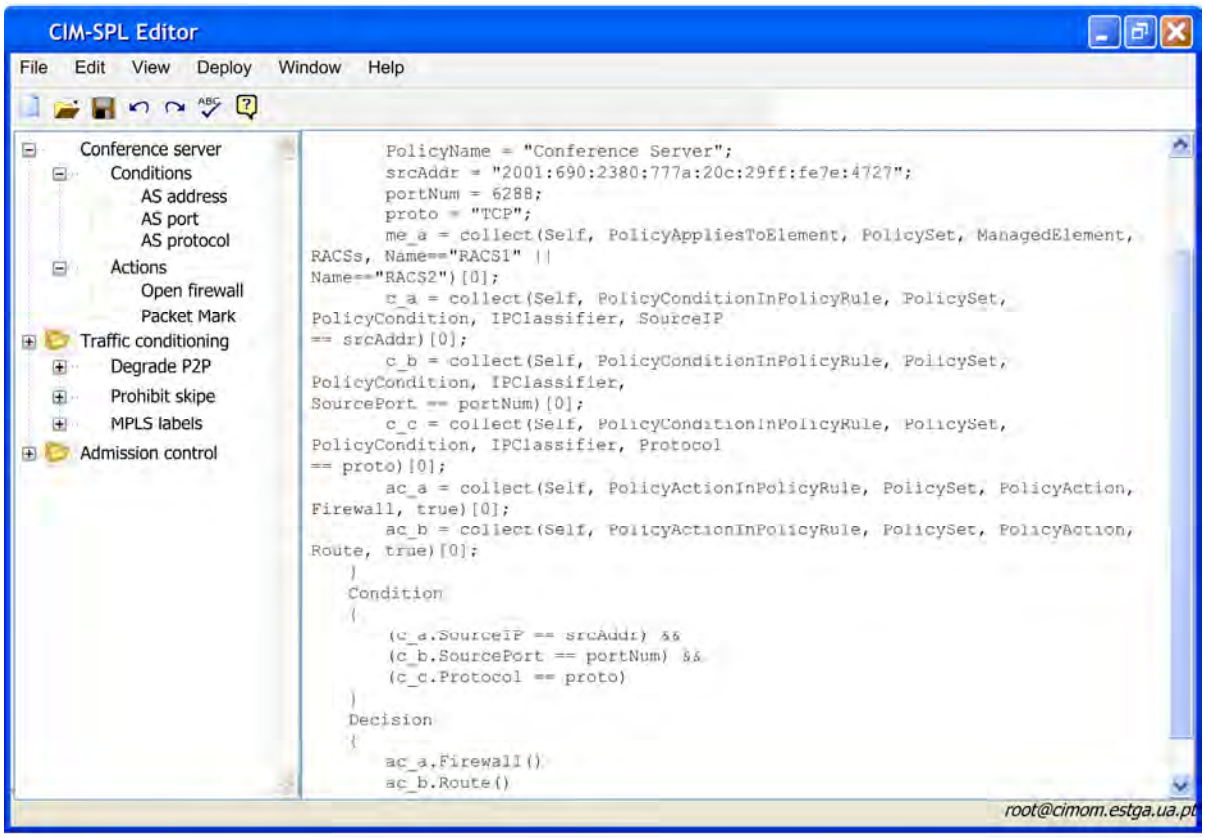

Figura 4.10 - Editor de SPL.

O editor inclui opções de compilação e execução de políticas que se encontram acessíveis através do menu *Deploy*. A compilação de políticas inclui uma verificação sintáctica, executada

através de um verificador desenvolvido com base no *parser* do projecto Apache Imperius [100]. As políticas sintacticamente correctas podem ser inseridas no repositório do CIMOM através da opção *Run*, caso contrário os erros sintácticos contidos na política são reportados ao administrador.

Ao contrário do que acontece na implementação do Imperius, as políticas não são executadas pelo editor, mas sim pelo servidor de gestão. Na implementação desenvolvida, assim que a política é transferida para o servidor de gestão, este inicia o processo de transferência desta para os elementos gestores intermédios através do adaptador de políticas. Esta diferença de implementação implicou uma restrição nos componentes da política aos objectos CIM, não permitindo métodos e propriedades Java disponíveis na plataforma de políticas do Imperius.

Com base nas extensões definidas para cada uma das componentes das políticas pode definir-se um vasto conjunto de políticas que se encontra exemplificado na Tabela 4.8. Podem ser escolhidos vários eventos, de entre os listados na Tabela 4.9, para desencadear a execução das políticas pela plataforma de gestão da rede, sendo que a ocorrência de um dos eventos definidos é suficiente para desencadear a verificação da política. A condição da política pode ser criada com base em qualquer um dos atributos das extensões às classes *CIM_PolicyCondition* desenvolvidas e ilustrados na Figura 10.1, tal como podem ser utilizadas qualquer uma das acções modeladas como extensões à classe *CIM_PolicyAction* na criação da componente de acção da política.

Tabela 4.8 - Exemplos de políticas.

DESCRIÇÃO	EVENTO	CONDIÇÕES	ACÇÕES	ELEMENTOS GERIDOS
Bloqueio de serviço	NullEvent	ServiceClass.ServiceClassID	Drop	RCEFss
Bloqueio a cliente	NullEvent	IPClassifier.SourceIP	Drop	RCEFs
Degradação de ligações P2P	NewReserv	IPClassifier.DestinationPort IPClassifier.Protocol	Shape Forward	RCEF
Degradação de serviço após ultrapassagem de limite de crédito	CreditThresh	IPClassifier.SourceIP ServiceClass.ServiceClassID	NullAction	RCEF
Remoção de etiquetas MPLS	NewReserv	MPLSClassifier.LabelStackID	RemoveLabel Shape Forward	RCEF
Sinalização RSVP	NewReserv	IPClassifier.DestinationIP IPClassifier.Protocol	CreateRSVPReserv Forward	RCEF
Reconfiguração da rede devido ao aumento de tráfego	LinkUtilThresh NOfSessPerLinkThresh CellUtilThresh	NullCondition	DegrLowerSessions	RCEF
Chamada de emergência	NewReserv	ServiceClass.ServiceClassID ServiceClass.Reserved LinkStatus.TotalBW LinkStatus.UsedBW	KillASession	RCEF
Pedido de configuração inicial de RCEF	ConfigElemReq	NullCondition	ConfigElement	RACS

A política que determina o bloqueio de um serviço de rede recebe como evento associado o *NullEvent*, determinando que deve ser continuamente executada. Ela especifica o serviço a

bloquear através do atributo *ServiceClassID* da classe *ServiceClass* e efectua o bloqueio através da execução do método *Drop*, aplicando-se a todos os elementos da rede instanciados da classe *RCEFs*. A definição da política que determina o comportamento da rede quando recebe uma chamada de emergência, é despoletada através do evento *NewReserv*. A identificação de que se trata de uma chamada de emergência é feita através da análise do atributo *ServiceClassID* da classe *ServiceClass*. A verificação da existência de recursos de rede suficientes para efectuar essa chamada é feita através da análise dos valores de *Reserved* da classe *ServiceClass*, bem como dos valores *TotalBW* e *UsedBW* da classe *LinkStatus*. Quando o gestor de políticas verifica a inexistência de recursos suficientes para o suporte da chamada de emergência, procede à interrupção de uma sessão existente invocando o método *KillASession*, e libertartando recursos suficientes para a chamada poder ser efectuada.

4.4 Comportamento dinâmico do sistema

Esta subsecção descreve aspectos relevantes acerca do comportamento dinâmico do sistema: os processos de distribuição da informação de configuração; a subscrição de eventos e definição de políticas; geração e tratamento de eventos; e o processo de execução de políticas.

4.4.1 Transmissão de informação de configuração

A configuração dos elementos de gestão é feita centralmente pelo administrador de sistema, através de uma aplicação gráfica que a insere no servidor de gestão, que por sua vez a dissemina por todos os elementos de gestão do sistema. Como a arquitectura do gestor é constituída por várias camadas, os elementos de cada uma efectuam a tradução e transmissão da informação para os elementos das camadas inferiores, de acordo com o processo ilustrado na Figura 4.11.

A definição da informação de configuração é feita pelo administrador do sistema no cliente gráfico de configuração, que por sua vez a insere no servidor central de gestão. O servidor efectua a inserção dessa informação no repositório central e transmite-a através do adaptador de configuração aos gestores de rede intermédios. Cabe ao adaptador efectuar a adaptação das mensagens WBEM e dos dados ao protocolo de comunicação implementado pelo gestor intermédio de rede. O gestor de rede armazena em seguida a informação de configuração no seu repositório interno e aplica no seu funcionamento a informação de configuração recebida. Dos elementos de configuração recebidos, são nesta fase extraídos os elementos relevantes para o funcionamento dos elementos de rede, que são adaptados ao protocolo de comunicação implementado pelos elementos de rede, e seguidamente transmitidos.

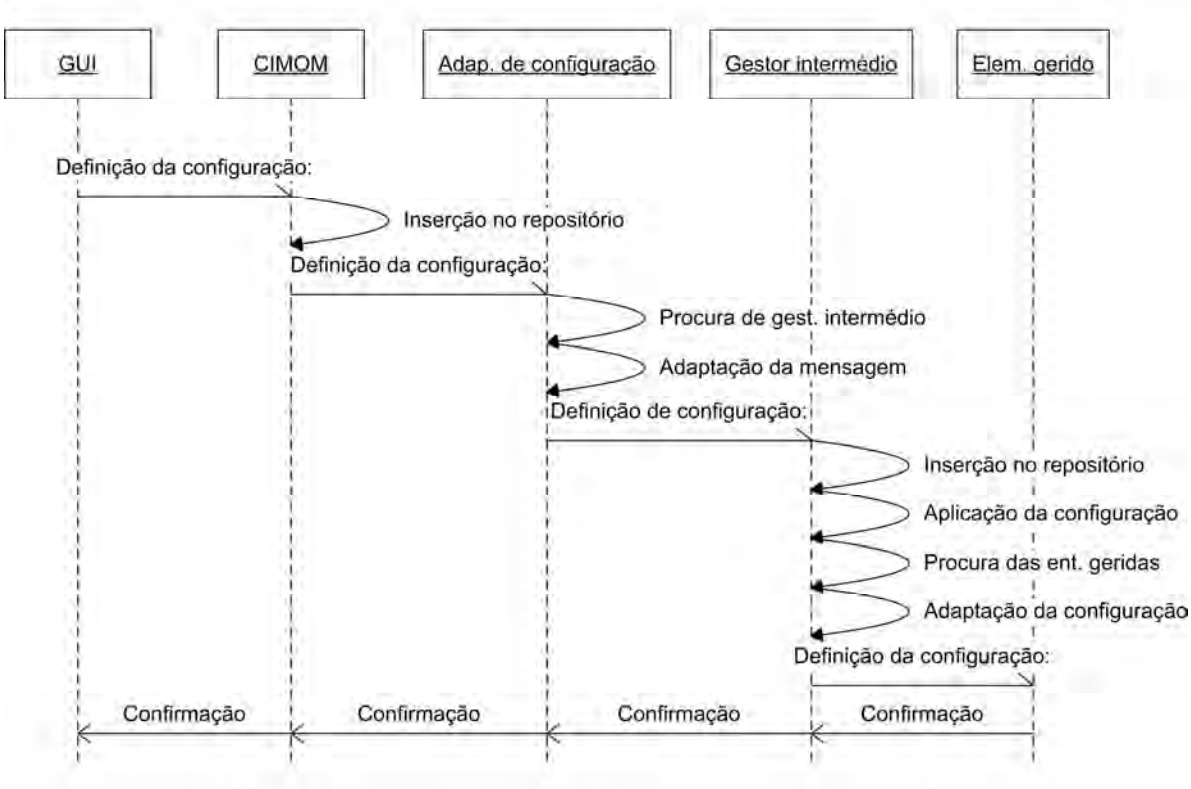

Figura 4.11 - Definição de informação de configuração.

4.4.2 Subscrição de eventos e aprovisionamento de regras

A adição de um evento que despoleta a execução de políticas obriga à criação de uma subscrição para a recepção do evento, por parte da entidade executora da política no processo de definição de políticas. A Figura 4.12 ilustra o processo de definição de políticas, bem como as interacções existentes entre os elementos participantes no processo.

As políticas são definidas pelo administrador do sistema através da interface gráfica. Esta transmite a informação que descreve a política ao gestor central da rede. A informação transmitida inclui:

- a indicação relativa ao evento desencadeador da avaliação da política;
- o conjunto de condições que devem ser verificadas para que a política seja executada;
- o conjunto de acções a executar;
- a lista dos elementos do cenário de gestão aos quais a política se aplica.

O gestor de rede armazena a informação no seu repositório interno e entrega a informação acerca da política ao adaptador de políticas. Este último verifica a consistência da política e informa o servidor central sobre o resultado do teste de consistência que armazena a informação no repositório central. Então o servidor central informa também o administrador da rede através da

aplicação gráfica. Reencaminha depois a informação relativa à subscrição da indicação ao adaptador de eventos, de forma a que este conheça a validade da subscrição e que possa efectuar filtragem dos eventos, de acordo com a metodologia descrita na subsecção 4.4.3. O adaptador de políticas armazena então a informação das políticas num repositório local, efectua a subscrição do evento relacionado com a política e determina quais os elementos gestores intermédios aos quais a política se aplica. Nesta fase faz-se a adaptação da informação da política aos elementos da camada intermédia, efectua-se a tradução da política para o protocolo de comunicação suportado pelos elementos em questão e envia-se a informação relativa à política para esses elementos.

O elemento gestor intermédio efectua: o armazenamento da informação no seu repositório local, a subscrição dos eventos relacionados com a política, o armazenamento da informação da subscrição, verificação de quais os elementos da sua rede que são afectados pela política, e a aplicação da política para que possa ser executada assim que for notificado da ocorrência do evento associado.

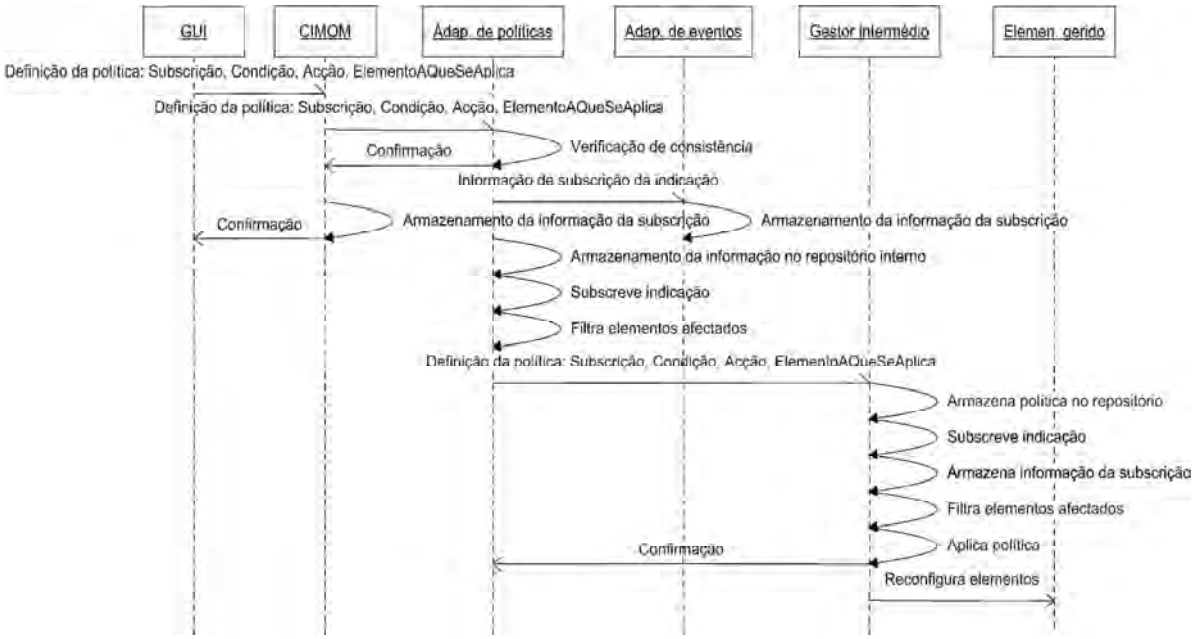

Figura 4.12 - Processo de aprovisionamento de políticas.

A informação relativa às políticas bem como a subscrição das indicações é feita local e centralmente, permitindo uma resposta da plataforma de gestão à ocorrência dos eventos, tal como se descreve na subsecção 4.4.4.

4.4.3 Geração e tratamento de eventos

A detecção de eventos e a reacção aos mesmos são cruciais para uma gestão eficaz da rede e dos serviços. Por um lado, permite autonomizar os elementos da plataforma de gestão visto que

passam a reagir à alteração do estado da rede segundo as regras que lhes são definidas através das políticas. Por outro, a existência de um conjunto de eventos que lhes são notificados assincronamente permite-lhes evitar o processo de verificação contínua dos valores das condições das políticas (que consumiria muitos recursos) permitindo assim aumentar a escalabilidade de toda a rede.

Os eventos processados pela plataforma de gestão passíveis de ser utilizados na especificação de uma política, encontram-se listados na Tabela 4.9, bem como o seu significado. Os eventos foram divididos em 4 grupos:

- um grupo de eventos genéricos que agrega o evento nulo, e eventos relacionados com o arranque e paragem dos elementos do sistema de gestão e são representados por objectos de classes derivadas de *MiscEvent*;
- um grupo de eventos relacionados com alertas internos do sistema, representados por objectos de classes derivadas de *CIM_AlertIndication*;
- um grupo de eventos relacionados com a criação e remoção de instâncias de vários objectos, representados em objectos de classes derivadas de *CIM_InstIndication*;
- e por último um grupo de eventos relacionados com a ultrapassagem de limiares de várias grandezas monitorizadas pelos elementos de gestão, representados como objectos de classes derivadas de *CIM_ThresholdIndication*.

Os eventos suportados pela plataforma, listados na Tabela 4.9, são tão diversos como a detecção de um pedido de nova reserva ou a notificação de que um gestor intermédio vai encerrar. Esta diversidade requer que a arquitectura da plataforma de gestão preserve a escalabilidade do sistema de gestão e que seja suficientemente flexível para suportar e processar as diversas origens dos diferentes eventos.

A plataforma de gestão proposta neste trabalho permite que a geração, a detecção e o processamento dos eventos sejam efectuados em qualquer das camadas da plataforma de gestão, aumentando a flexibilidade e escalabilidade da mesma. Eventos como a detecção de novas reservas devem ser interceptados ao nível das entidades de rede e processados ao nível dos gestores intermédios. Um elemento de rede recebe vários pedidos de reserva por segundo, não podendo ser processados centralmente sob pena de comprometer a escalabilidade do sistema, num cenário de uma rede de um operador de telecomunicações. Alguns eventos como os que avisam do encerramento de um gestor intermédio devem ser notificados por esse gestor e processados centralmente; o número de gestores intermédios permite o seu processamento central sem que seja comprometida a escalabilidade da solução. Adicionalmente, o processamento central de eventos relacionados com elementos gestores intermédios permite que sejam implementados mecanismos de verificação da configuração dos gestores durante o arranque.

Tabela 4.9 - Lista de eventos detectados pela plataforma de gestão.

TIPO DE EVENTO	NOME DO EVENTO	DESCRIÇÃO
MiscEvent	NullEvent	Evento que serve para indicar a verificação contínua de uma política.
	AfterStartup	Evento que activa execução de políticas antes do encerramento do servidor de gestão central.
	BeforeShutdown	Evento que despoleta a execução de políticas depois do arranque do servidor de gestão central.
	AfterMLEStartup	Evento que despoleta a execução de políticas antes do encerramento de gestor intermédio.
	BeforeMLEShutdown	Evento que despoleta a execução de políticas depois do arranque de gestor intermédio.
CIM_AlertIndication	LinkDown	Criado quando elementos da camada de rede detectam a perda de uma ligação de rede.
	LinkUp	Semelhante ao evento anterior para situações de recuperação da ligação.
	ElemDown	Detectado pelo gestor intermédio quando elemento da camada de rede deixa de responder.
	ElemUp	Semelhante ao anterior quando elemento de rede arranca.
CIM_InstIndication	NewReserv	Criado quando uma reserva de serviço é pedida.
	ChangeReserv	Criado quando uma reserva de serviço é alterada.
	EraseReserv	Criado quando uma reserva de serviço é removida.
	NewAuthorization	Criado quando novo pedido de autorização é feito.
	EraseAuthorization	Criado quando autorização é removida.
	ConfigNATReq	Criado quando é recebido pedido de abertura de um porto no servidor de NAT.
	ConfNetElemReq	Pedido de configuração de elemento de rede.
CIM_ThresholdIndication	LinkUtilThresh	Evento criado quando a ligação ultrapassou um limite predefinido.
	CreditThresh	Evento criado quando o utilizador ultrapassou um limite predefinido de crédito. (*e.g.:* utilização em serviços pré-pagos).
	NOfSessPerUserThresh	Evento criado quando o número de sessões permitido pelo contrato do utilizador ou pelo operador é ultrapassado.
	NOfSessPerServThresh	Semelhante ao evento anterior, mas relativo ao número de serviços.
	NOfSessPerLinkThresh	Semelhante ao evento anterior, mas relativo ao número de serviços por ligação.
	CellUtilThresh	Evento gerado quando a carga em célula ultrapassa determinado limite predefinido.
	FraudDetec	Gerado com base na suspeita de fraude na utilização dos recursos de rede.

A Figura 4.13 ilustra a sequência de mensagens trocadas entre as entidades envolvidas no processamento de eventos da plataforma de gestão. Quando uma entidade de rede detecta a ocorrência de um determinado evento informa o gestor intermédio. Este verifica se possui alguma subscrição desse tipo de evento, processa-o e gera uma indicação que envia ao adaptador de eventos.

O adaptador de eventos repete o processo implementado pelo gestor intermédio: lê as subscrições, processa a indicação enviada pelo gestor intermédio e gera uma nova indicação que envia ao gestor de eventos do servidor central. A partir daí o gestor central encarrega-se de

notificar os elementos do cenário de gestão que previamente tinham subscrito essas indicações, de acordo com o processo descrito em 4.4.4.

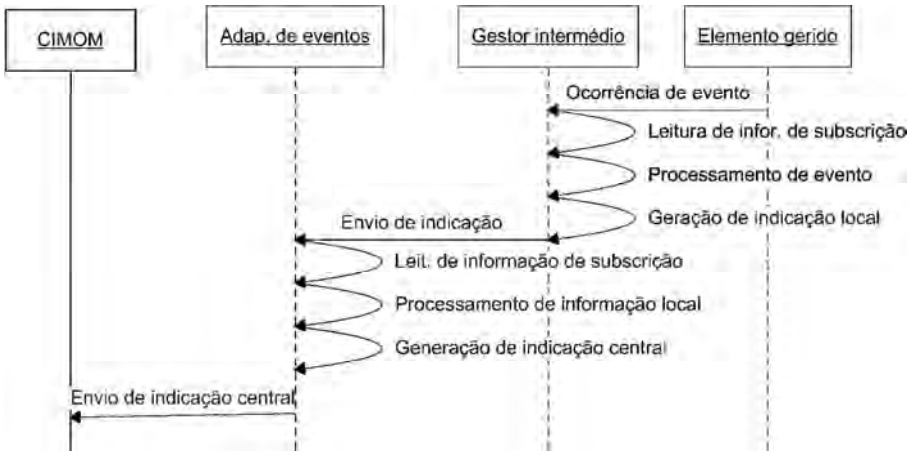

Figura 4.13 - Sequência de processamento de eventos.

O processamento dos eventos levado a cabo pelo gestor intermédio e pelo adaptador de políticas é realizado de acordo com o diagrama de actividades ilustrado na Figura 4.14. Quando recebem um evento, efectuam uma procura no repositório local em busca de uma subscrição de um evento semelhante. Caso não seja encontrada nenhuma subscrição, o evento é descartado e o processo volta a esperar a recepção de novo evento. Sendo encontrada uma subscrição é feita a sua análise. Como a subscrição é representada como um objecto da classe de associação CIM do tipo *IndicationSubscription*, inclui informação acerca do tempo de validade da subscrição e do tempo entre notificações de eventos semelhantes.

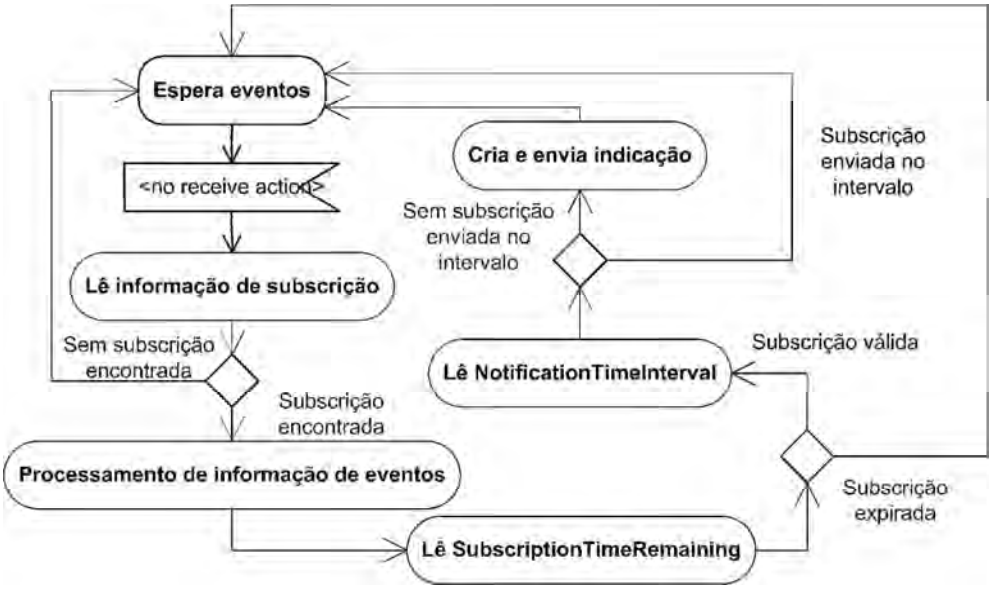

Figura 4.14 - Processamento de eventos.

Depois de processada a informação acerca da subscrição é verificado o tempo de validade da mesmas. Se já não for válida, o processo é abortado voltando o sistema a esperar novos eventos para processar. Confirmando-se a validade da subscrição é verificado se foi enviada alguma indicação acerca do evento no período entre indicações definido pela propriedade *NotificationTimeInterval* da subscrição. Não tendo sido ainda enviada nenhuma indicação, é gerada uma e enviada, caso contrário o sistema ignora o evento recebido e volta a esperar a chegada de novos eventos.

4.4.4 Execução das políticas

A arquitectura proposta permite a divisão das políticas em duas classes: políticas estáticas, que obrigam o elemento executor a monitorizar continuamente as suas condições; e políticas com um carácter mais dinâmico, que são analisadas em resposta a um evento externo ao sistema de gestão. As primeiras são especificadas sem que seja definido qualquer elemento na componente dos eventos e são entregues ao elemento gestor, que continuamente verifica a validade das suas condições e que está encarregue de as executar. Às segundas é associado um evento que é utilizado na definição de uma subscrição que garante que na sua ocorrência a entidade executora da política será notificada.

As políticas podem ainda ser executadas de duas formas distintas: centralmente pelo gestor, ou localmente pelos elementos gestores intermédios da rede. Esta característica aumenta a flexibilidade da arquitectura de gestão: por um lado permite tornar a solução de gestão mais escalável, uma vez que é delegada alguma responsabilidade nos elementos de gestão intermédios, permitindo que estes decidam sem depender em tempo real do gestor central; por outro permite concertar centralmente a execução de políticas que dependam de vários gestores, implementando por exemplo mecanismos de verificação de consistência e controlo transaccional. Como exemplo pode-se pensar numa política que altere as características de um serviço de rede, alterando tanto o tratamento dos pacotes como o preço cobrado pelo serviço. Uma regra deste tipo exige uma alteração concertada entre os elementos gestores dos utilizadores e os elementos gestores de recursos da rede, de modo a alterarem os mecanismos de registo de utilização, e simultaneamente reconfigurar os equipamentos de rede. A Figura 4.15 ilustra o processo de execução de políticas definindo as interacções existentes entre as entidades intervenientes no processo.

Quando é detectado um evento, quer ao nível da rede quer centralmente, é feita a notificação dessa ocorrência para as entidades subscritoras. Ao nível da rede, os eventos são detectados pelos elementos de rede que notificam o elemento gestor intermédio. Este procura no repositório interno as políticas relacionadas com a indicação em questão e reencaminha a indicação

para o adaptador de eventos. Avalia então as condições das políticas encontradas e executa as acções relacionadas com as políticas.

Quando o adaptador de eventos recebe a indicação, processa-a de acordo com a metodologia definida na secção 4.4.3 e gera uma nova indicação que envia ao gestor de eventos existente no servidor de gestão central. De acordo com o definido no modelo de gestão de eventos do DMTF [30], e implementado na maioria das implementações WBEM [22, 23], o gestor de eventos procura subscritores das indicações em questão e notifica-os da ocorrência desses eventos. Notifica também o adaptador de políticas para que este possa executar alguma política de âmbito global que possa existir.

As respostas do adaptador de políticas e do elemento de gestão intermédia são em tudo semelhantes: procuram nos repositórios internos a existência de políticas associadas com a indicação de que foram notificados; analisam as condições das políticas que obtiveram, e executam as acções constantes nas políticas cujas condições consideraram verdadeiras.

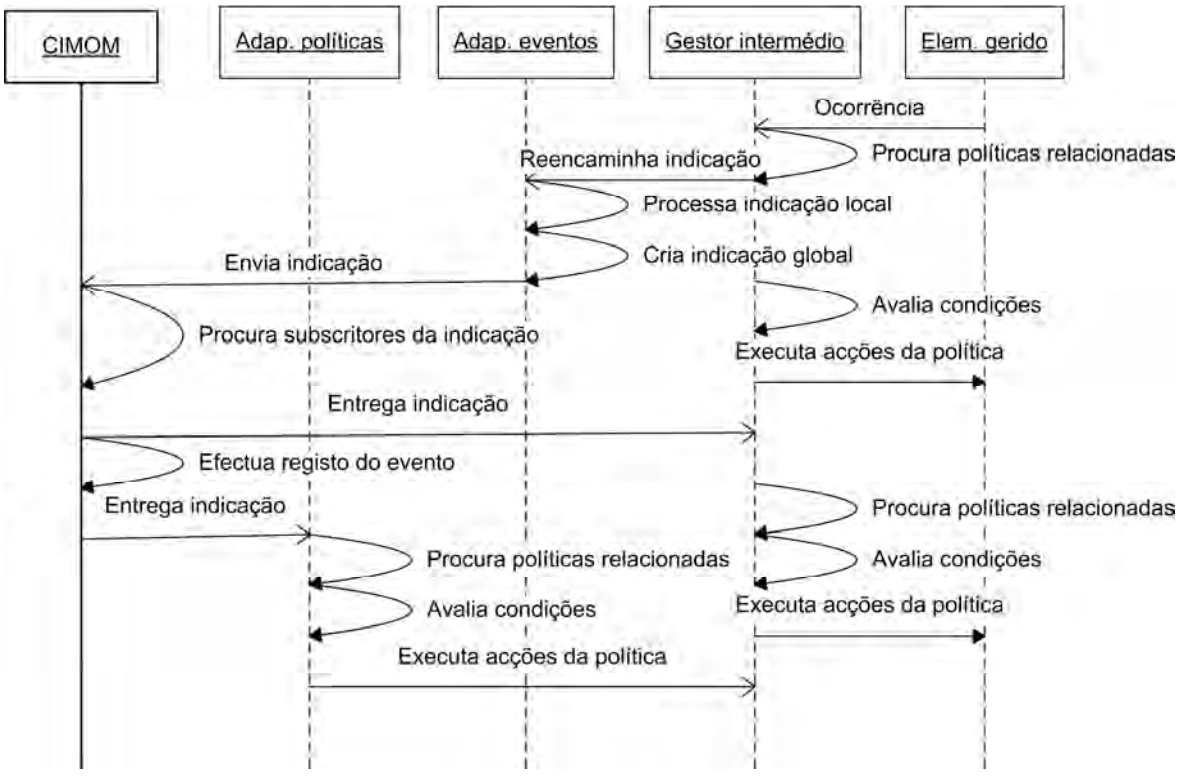

Figura 4.15 – Processo de execução de políticas.

O adaptador de políticas faz ainda registo da ocorrência das indicações, de forma a permitir ao administrador, através da interface gráfica do sistema, verificar os eventos relacionados com o gestor central do sistema que tenham ocorrido. A consulta desses eventos permite ao administrador

do sistema tomar decisões relacionadas com a especificação de novas políticas, alteração das políticas existentes ou ainda com aspectos relacionados com a segurança e planeamento da rede.

4.5 Implementação

No desenvolvimento da solução de gestão descrita na secção 4.2 foram utilizados vários componentes previamente desenvolvidos. A Figura 4.16 ilustra a origem desses componentes.

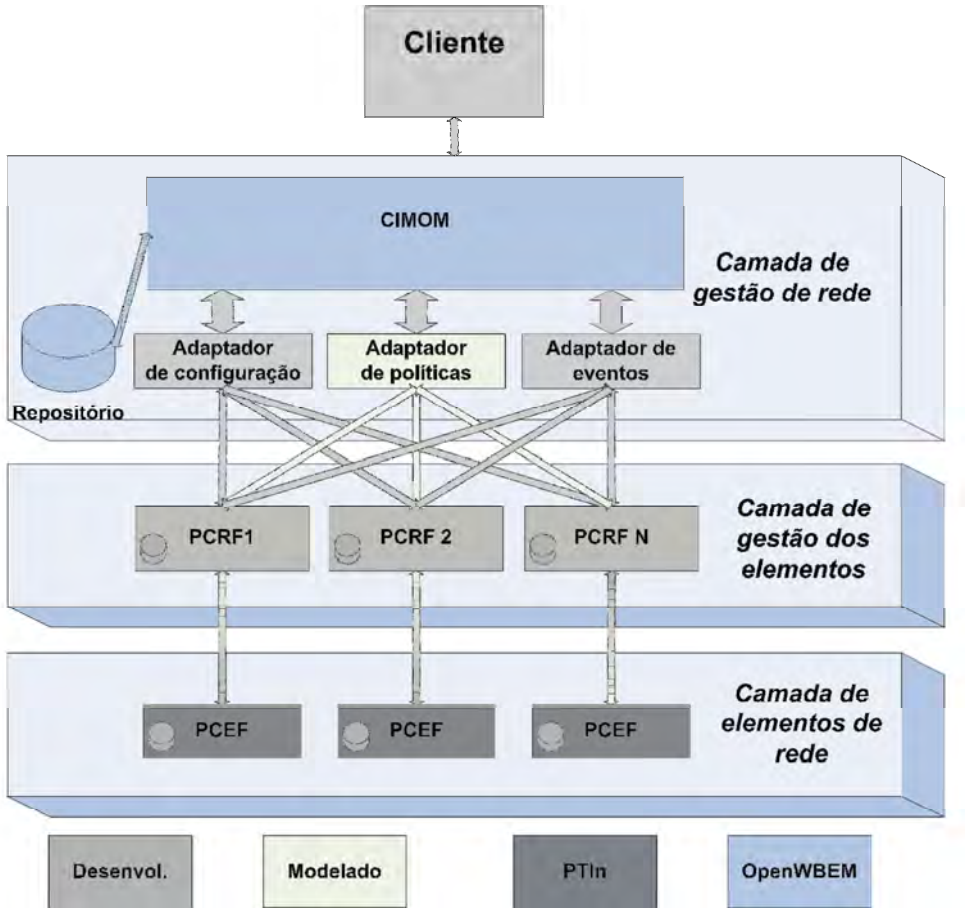

Figura 4.16 – Origem dos vários componentes utilizados.

A consola de gestão [101] é uma aplicação gráfica desenvolvida em Java que utiliza a API Sun WBEM SDK [102] para interligação com o servidor de gestão. A verificação sintáctica das políticas SPL, bem como a compilação das mesmas é feita recorrendo a componentes desenvolvidos baseados no projecto Apache Imperius [100].

O servidor central de gestão e o repositório de políticas foram implementados com base no servidor CIM OpenWBEM. Foram desenvolvidos adaptadores na linguagem de programação C++, com base na API fornecida pelo servidor de gestão. Foi reutilizado o repositório da informação

(base de dados relacional DB2) desenvolvido no âmbito do projecto OpenWBEM como repositório central da solução de gestão.

As extensões efectuadas ao modelo CIM foram efectuadas através da criação de ficheiros MOF, que posteriormente foram compilados. As classes foram inseridas no servidor de gestão através de uma aplicação designada de *owmofc* que é fornecida em conjunto com a plataforma de desenvolvimento do OpenWBEM.

Os adaptadores de gestão que interligam os elementos da camada intermédia foram desenvolvidos em C++ tendo sido utilizada uma API NETCONF [103] para efectuar a implementação do cliente NETCONF.

Os elementos da camada intermédia utilizados são protótipos do produto *ip-rudder* desenvolvido pela PT Inovação no âmbito da solução IMS da empresa [104], tal como algumas aplicações que emulavam os elementos da camada de rede.

4.6 Sumário

Nesta secção foi apresentada uma arquitectura de gestão de rede da próxima geração. Ao longo deste trabalho foi identificado o conjunto de requisitos de gestão, e foram efectuadas propostas para a arquitectura da solução de gestão, para o modelo de dados e para a metodologia de configuração da solução de gestão apresentada.

A arquitectura proposta é constituída por três camadas e segue o modelo de gestão definido pelo 3GPP. O gestor central foi implementado com recurso a um servidor de gestão baseado na tecnologia WBEM tendo sido desenvolvido um conjunto de adaptadores que efectuam a adaptação da informação de gestão, de acordo com a capacidade dos elementos da camada intermédia.

Relativamente à componente de politicas, foi proposta uma estrutura de políticas dotada de uma componente dinâmica, bem como uma plataforma para a sua execução que permite ao sistema de gestão responder à ocorrência de eventos na rede, autonomizando o comportamento do sistema de gestão.

A metodologia de configuração da solução de gestão proposta consiste na utilização de uma aplicação gráfica pelo administrador da rede, que permite a gestão centralizada de todos os sistemas que compõem a rede. A aplicação permite ainda a definição dos parâmetros relativos aos serviços e aos recursos de rede disponíveis, bem como das políticas que determinam o comportamento dos sistemas.

O carácter hierárquico e distribuído da solução proposta permite, por um lado que as acções de configuração sejam distribuídas por todos os elementos gestores intermédios, evitando os constrangimentos associados a um único elemento responsável pela configuração de todos os

equipamentos da rede; e por outro lado que possam ser definidos pelo administrador quais os elementos que devem correr cada uma das políticas, determinando se estas devem ser executadas central ou localmente.

5 Análise do sistema de gestão

Nesta secção são analisados os resultados da solução de gestão proposta na secção anterior. Inicialmente é analisado o processo de escolha do servidor de gestão utilizado na criação do servidor central de gestão. Seguidamente é analisado individualmente o desempenho de cada uma das entidades que constituem o sistema de gestão e é ainda comparado o desempenho das tecnologias de gestão utilizadas no desenvolvimento do sistema com o desempenho de tecnologias de gestão alternativas. Finalmente é dimensionada a solução global de gestão e é analisada a sua escalabilidade, de forma a poder concluir da adequabilidade do modelo proposto a uma rede de grande dimensão, equivalente a um operador de comunicações.

5.1 Escolha do servidor central de gestão.

O servidor central de gestão foi desenvolvido recorrendo à utilização da tecnologia WBEM. Atendendo ao facto de existirem várias implementações de código aberto baseadas nesta tecnologia, foram analisadas as alternativas existentes com o objectivo de escolher a implementação mais adequada para o desenvolvimento do servidor. Assim, foram avaliadas implementações, tais como OpenWBEM, OpenPegasus, SBLIM e WBEMServices, relativamente a vários aspectos, tais como a arquitectura, o envolvimento da comunidade de software livre, o suporte disponibilizado ao projecto, a adopção do projecto pela indústria e o desempenho do mesmo. A Tabela 5.1 mostra os dados resultantes da análise das várias soluções.

Para determinadas características das implementações estudadas foi aplicada uma escala de classificação com valores entre 0 e 5 (em que 0 representa a classificação mínima e 5 a classificação máxima), que pretende representar o resultado da avaliação relativa a cada uma das características.

Em termos de arquitectura, todas as implementações demonstraram ser interessantes pelo facto de suportarem o desenvolvimento de soluções de gestão distribuída e de a sua utilização ser independente do sistema operativo. Todos os servidores foram desenvolvidos em linguagens de programação vulgares para os quais é simples obter um compilador para qualquer sistema operativo.

Tabela 5.1 - Comparação das implementações.

CARACTERÍSTICA	OPENPEGASUS	WBEMSERVICES	SBLIM	OPENWBEM
Arquitectura				
Linguagem de desenvolvimento	C++	Java	C	C++
Integração em sistemas operativos	Qualquer	Qualquer	Qualquer	Qualquer
Adaptadores remotos	Sim	Sim	Sim	Sim
Envolvimento da comunidade				
Envolvimento da comunidade de desenvolvimento (1= inexistente..5= muito forte)	4	2	3	4
Dinamizador	IBM, HP e EMC	Sun	IBM	Novell Vintella
Suporte do projecto				
Aplicações de suporte (1= nenhuma..5= muitas)	4	4	2	4
Documentação (1= nenhuma..5= muita)	4	3	4	3
Mailing lists (1= muito pobres..5= bastante utilizada)	4	4	4	4
Adopção do projecto				
Empresas que utilizam implementações open source	HP	Sun	IBM	Novell
Produtos comerciais baseados na implementação	HP-UX SDK SSP Software Technologies	WBEM services	IBM-AIX	Vintela Management Extensions AppleRemote Desktop 2 Novell / SuSE SLES 9
Desempenho				
Tempo de resposta (1= péssimo..5= excelente)	2	1	Não avaliado	4
Requisito de memória (1= pesado..5= leve)	3	1	Não avaliado	4

Todos os projectos eram dinamizados por importantes fabricantes de software e obtiveram um envolvimento da comunidade de software aberto, com dezenas de pessoas a contribuir para o desenvolvimento, a detecção e a correcção de erros.

Em termos de suporte do projecto, observou-se que o OpenWBEM apresentava maior número de aplicações de suporte, mas que OpenPegasus e SBLIM apresentavam melhor documentação, tanto na forma de guias de instalação como de documentação de apoio ao desenvolvimento de software. Da avaliação da comunidade nas listas de discussão verificou-se que todos os projectos possuíam uma grande participação da comunidade para o apoio mútuo.

Todos os projectos deram origem a produtos de gestão comerciais, especialmente pela parte da empresa dinamizadora, pelo que foi considerado que existia uma forte adopção do projecto por parte da indústria para todos os projectos.

Relativamente à quantidade de aplicações de apoio oferecidas, salientou-se o projecto OpenWBEM.

Dos parâmetros avaliados aquele em que foi encontrada uma maior disparidade de resultados foi o desempenho. Em [105] são avaliados os requisitos de memória, dos servidores OpenPegasus e OpenWBEM, onde se mostra que OpenWBEM é significativamente mais eficiente na utilização de memória do que o OpenPegasus. Estes resultados foram confirmados num outro estudo [106], onde é demonstrado além disso que WBEMServices requer aproximadamente o triplo da memória de OpenPegasus e o quádruplo de OpenWBEM.

Em termos de tempo de resposta, o OpenWBEM requer aproximadamente metade do tempo que o OpenPegasus e um quarto do tempo do WBEMServices para a generalidade das operações [106], resultados que vêm em linha com os resultados publicados por Zeng et al. em [107].

Em função dos parâmetros avaliados, especialmente os que se relacionam com o desempenho do servidor, foi escolhida a solução OpenWBEM como base de desenvolvimento do servidor de gestão.

5.2 Desempenho dos elementos do sistema de gestão

Nesta secção é analisado o desempenho dos vários elementos pertencentes ao cenário de gestão. São descritos os testes realizados para efectuar a avaliação do tempo de resposta, da memória ocupada pelos sistemas computacionais, bem como da largura de banda de sinalização produzida durante o funcionamento dos vários elementos do cenário. São adicionalmente testadas várias tecnologias de gestão alternativas e são comparados os resultados com os resultados obtidos pelas tecnologias utilizadas.

5.2.1 Desempenho do servidor central de gestão

O desempenho do servidor central de gestão tem a maior importância para o comportamento global da rede pelo facto de efectuar a gestão global da rede. A presente secção avalia o desempenho do servidor central em termos de memória utilizada, volume de sinalização produzida e tempo de resposta.

Descrição da plataforma de testes

A plataforma de testes de avaliação de desempenho do servidor central de gestão consistiu na utilização do servidor do projecto OpenWBEM designado de *owcimomd* e de um cliente do mesmo projecto designado de *owxecwql*. O cliente no seu arranque efectua um pedido de configuração à aplicação servidora para efectuar a enumeração dos elementos de uma classe. A aplicação servidora, que previamente efectuava a leitura da informação de uma base de dados

relacional, envia-a à aplicação cliente. A estrutura dos elementos de configuração trocados está identificada na Tabela 5.2 e representa a informação que descreve cada uma das interfaces dos elementos de rede, que tipicamente é trocada entre o servidor de gestão central e o elemento gestor da rede. Foram realizadas várias experiências com diferentes quantidades de elementos, que eram estrategicamente colocados na base de dados de forma a analisar a evolução do comportamento do servidor face às variações do volume de informação.

Tabela 5.2 – Descrição do objecto de configuração Interface.

ELEMENTO	TAMANHO	DESCRIÇÃO
InterfaceID	2	Chave da entidade
Address	4	Endereço IPv6
Bandwidth	2	Total de largura de banda
Uplink	2	Interface Uplink ou Downlink
NetworkID	2	Rede a que pertence a interface
Prefix	2	Tamanho do prefixo IPv6
PrefixADDR	4	Prefixo IPv6
BWunit	2	Unidade de largura de banda
IfIndex	2	Índice interno ao *router*

A comunicação entre as aplicações utilizadas era efectuada através de uma rede Fast-Ethernet dedicada, de modo a remover a interferência causada por outro tráfego de rede. O tráfego existente na rede provocado pela comunicação entre as aplicações foi capturado e analisado, com o objectivo de medir o volume de informação trocada entre o cliente e o servidor, bem como o tempo de comunicação necessário à troca de informação. Durante as experiências foi também monitorizada a aplicação servidora com o objectivo de medir a quantidade de memória máxima usada durante o processo de troca de mensagens. Os testes foram realizados várias vezes, para possibilitar o cálculo de valores médios de cada uma das grandezas.

Para efectuar os testes foram utilizadas duas máquinas com o sistema operativo *Ubuntu linux* com o kernel 2.6.22, com as seguintes características:

- Servidor: Intel Dual core a 1.8 GHz com 512 MB RAM;
- Cliente: Centrino Intel 1.7 GHz com 1GB RAM.

Análise de resultados

A quantidade de informação trocada entre o cliente e o servidor cresce linearmente com o aumento da quantidade de registos na base de dados. Da análise da Figura 5.1, pode-se verificar que para 10000 objectos trocados o servidor gera aproximadamente 10 Gbit de sinalização.

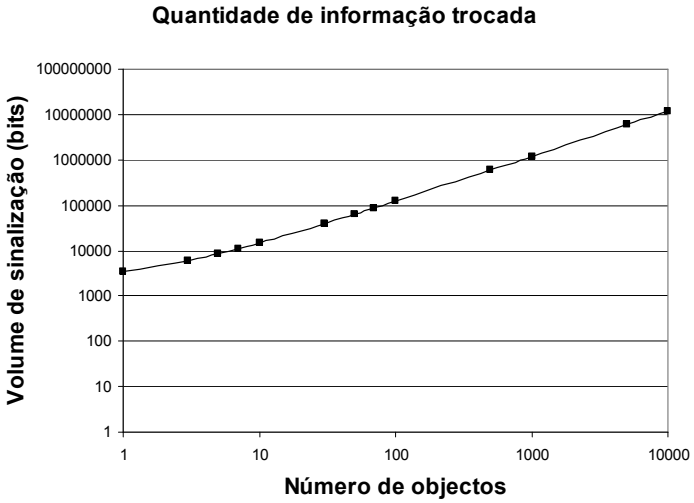

Figura 5.1 - Quantidade de informação trocada pelo servidor.

O tempo de resposta do servidor (Figura 5.2), manteve a tendência verificada em relação à quantidade de informação, ou seja, de existir um crescimento aproximadamente linear com o aumento do número de registos colocados na base de dados. A troca de 1000 objectos efectua-se em cerca de 0,8 segundos, enquanto que a troca de 10000 registos se processa num período de pouco mais de 8 segundos.

Figura 5.2 - Evolução do tempo de resposta do servidor com o aumento de informação.

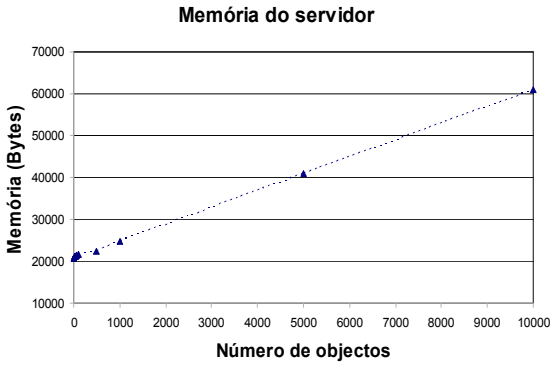

Figura 5.3 - Evolução da utilização da memória do servidor com o aumento de informação.

Em termos de memória ocupada pelo servidor (Figura 5.3), verificou-se que tem um valor inicial de cerca de 20 KByte e que aumenta linearmente com o crescimento do número de registos. Durante o processo de troca de 10000 objectos, verificou-se que a aplicação servidora ocupou cerca de 60 KByte de memória. Relacionando o incremento na utilização de memória com a quantidade de informação trocada pelo servidor, verificamos que este é cerca de 310 vezes maior do que o seu armazenamento em memória. A justificação desta diferença prende-se com o facto de a informação

ser armazenada em memória de uma forma mais compacta, evitando as sobrecargas causadas pelas *tags* XML e a sobrecarga dos cabeçalhos dos protocolos de transporte da informação.

5.2.2 Desempenho da interface com os gestores intermédios

A interface com gestores intermédios é essencialmente utilizada como meio de configuração dos elementos da camada intermédia de gestão. A frequência das mensagens será relativamente baixa, mas essas mensagens terão dimensões consideráveis visto transportarem a informação de configuração dos elementos da camada intermédia.

Esta secção descreve os testes e resultados da avaliação de desempenho das tecnologias envolvidas no desenvolvimento da interface de comunicação com os elementos de gestão intermédia: tecnologia WBEM, NETCONF e Diameter. Os testes efectuados mediram os requisitos de sinalização dos protocolos de comunicação das tecnologias, os requisitos de memória das entidades envolvidas na comunicação, e o número de mensagens necessárias à comunicação. Foi ainda efectuado um estudo analítico, com base na informação retirada dos RFCs e especificações do DMTF, acerca de cada uma das tecnologias, onde se previu o seu comportamento nos testes realizados através de uma simulação. Foram posteriormente comparados os dados provenientes da simulação com os dados provenientes dos testes, de forma a eliminar possíveis erros provenientes de especificidades das implementações utilizadas nos testes.

Foram ainda testadas tecnologias de gestão alternativas como SNMP, COPS e *Web Services* e comparados os dados das suas performances com os das tecnologias utilizadas para o cenário de gestão em estudo.

Descrição da plataforma de testes

Nos testes de avaliação do desempenho das interfaces foi colocada a aplicação gestora central numa máquina e o elemento gestor intermédio noutra (Figura 5.4). Foram interligadas por um segmento de rede FastEthernet isolado da restante rede, de forma a evitar que outro tráfego de rede pudesse interferir com o tráfego trocado entre ambas as aplicações de gestão. Foi então capturado o tráfego trocado entre as duas aplicações.

A plataforma de testes usada durante os testes de comparação de tecnologias consistiu num par de aplicações desenvolvidas segundo o paradigma cliente / servidor em que o cliente no seu arranque efectua um pedido de configuração à aplicação servidora. Esta, que previamente efectuava a leitura da informação de uma base de dados relacional, envia-a à aplicação cliente. Foram criadas várias aplicações, e um par cliente/ servidor por cada uma das tecnologias:

- Foram desenvolvidos um servidor e um cliente Diameter com as funcionalidades mínimas, interligados por uma interface que implementava as especificações definidas nas RFC 3588 e 5224;
- Foram desenvolvidos um servidor e um cliente COPS com as funcionalidades mínimas, interligados por uma interface baseada na API *COPS++* [108] que implementava as especificações definidas na RFC 2748;
- Foi desenvolvido um agente SNMP com as funcionalidades mínimas, que implementava uma interface baseada na API *SNMP++* [109]. A consola de gestão utilizada pertence ao pacote *Net-SNMP*. A versão do protocolo utilizada foi SNMPv2, dado que SNMPv1 não permite utilizar mecanismos de troca de informação em bloco e que SNMPv3 não é muito utilizado em cenários de gestão [110];
- Foi utilizada uma versão de *OpenWBEM* como aplicação servidora de WBEM (*owcimomd*) e a aplicação designada de *owexecwql* também incluída no pacote, como aplicação cliente;
- Foi utilizada uma versão de *Openwsman* [111] como aplicação servidora de WS-Management (*openwsmand*) e a aplicação designada de *wsman*, também incluída no pacote, como aplicação cliente;
- Foram desenvolvidos um servidor e um cliente NETCONF com o mínimo de funcionalidades, e foram interligados por uma interface baseada na API *Yenca* [103] que implementa as especificações definidas na RFC 4743.

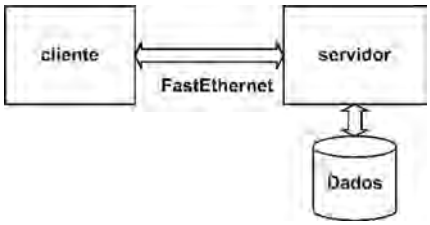

Figura 5.4 - Arquitectura geral da plataforma de testes

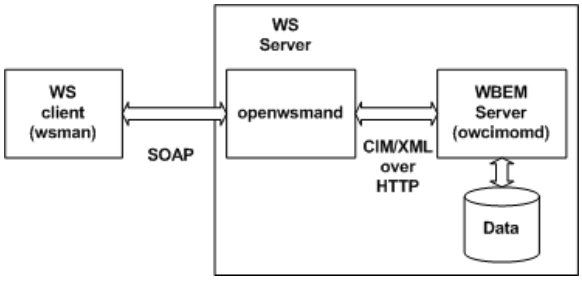

Figura 5.5 - Arquitectura da plataforma de testes para a tecnologia WS-Management.

A implementação WS-Management do projecto *Openwsman* utiliza o servidor *OpenWBEM* como servidor CIM, actuando o servidor *Openwsman* (*wsmand*) como um cliente do servidor *OpenWBEM* (*owcimomd*), tal como ilustrado na Figura 5.5. Durante as experiências relativas à tecnologia WS-Management, ambos os servidores foram colocados na mesma máquina e as

capturas de tráfego foram efectuadas de forma a registar o tráfego entre o cliente e o servidor *Openwsman.*

A Tabela 5.3 sumaria as principais características das aplicações utilizadas na plataforma de teste. Durante os testes, o tráfego de rede entre o cliente e o servidor foi capturado. Estas capturas foram analisadas, tendo sido contado o número de pacotes, o número de bytes, verificado o tamanho dos cabeçalhos e o tamanho das mensagens do cliente. Os testes foram repetidos várias vezes e foram calculadas as médias das várias grandezas.

Tabela 5.3 - Sumário das características das aplicações de teste.

TECN.	TIPO DE APLICAÇÃO	INTERFACE	VERSÃO	MENSAGENS	
				NOME	TAM
SNMP	Agente simples e consola net-snmp	Baseda em Agent++	RFC 1441	getBulkRequest	87
				get-Response	*
COPS	Servidor e cliente criados para teste	Baseda em COPS++	RFC 2748	REQ	126
				DEC	*
				RPT	120
Diameter	Servidor e cliente criados para teste	Baseda numa API Diameter	RFC 3588 RFC 5224	RAR	214
				RAA	*
WBEM	Versão simplificada de OpenWBEM como servidor e owexecwql como cliente	OpenWBEM	CIM Operations over HTTP – v 1.3.0	EnumerateInstances	884
					*
WSMAN	Versão simplificada de OpenWsman como servidor e wsman como cliente	Openwsman	Web Services for Management (WS-Management) Specification	wsen:Enumerate	935
				wsen:EnumerateResponse	*
NETCONF	Servidor e cliente criados para teste	Yenca	RFC 4743	get-config	409
				config	*

As mensagens trocadas durante os testes seguem o cenário descrito no início da secção:

- O cliente SNMP pede configuração ao servidor utilizando mensagens *getBulkRequest*; este responde através de mensagens *getResponse*, sendo as mensagens mais frequentes entre o tráfego de gestão SNMP [110];
- O cliente COPS envia uma mensagem *REQ* com 126 bytes pedindo a configuração do servidor; este responde com uma mensagem *DEC* onde inclui a informação de gestão, seguindo o comportamento típico das entidades de um cenário COPS-PR. O cliente confirma a recepção da resposta com uma mensagem *RPT* com 129 bytes, reportando o sucesso de instalação da decisão recebida;
- O cliente Diameter pede a configuração através de uma mensagem *RAR* com 214 bytes e recebe a resposta do servidor através de uma mensagem *RAA*;
- O cliente WBEM pede a sua configuração através de uma mensagem *EnumerateIntances* com 884 bytes e recebe a resposta *EnumerateIntancesResponse* do servidor;

- O cliente WS-Management pede a configuração através de uma mensagem *Enumerate* com 935 byte e recebe a resposta do servidor através de uma mensagem *EnumerateResponse*;
- O cliente NETCONF pede a configuração ao servidor através de uma mensagem get-config com 409 bytes e este responde com uma mensagem *config*.

O tamanho da mensagem de resposta varia com a quantidade de informação trocada, devido ao facto de ser essa mensagem que transporta a informação de gestão trocada entre as duas entidades.

Dado que nem todos os tipos de dados são trocados com a mesma frequência entre as entidades de gestão, nas experiências efectuadas foram executados testes para cada um dos tipos de dados em separado. Foi posteriormente tido em conta o efeito de cada um dos componentes, segundo a frequência observada por Schönwälder [110] e apresentada na Tabela 5.4.

Tabela 5.4 – Frequência de cada tipo de dados em informação de gestão.

TIPO	FREQUÊNCIA
Byte	23
Integer	66
Address	4
String	8

A grande maioria dos dados trocados nas mensagens de gestão (cerca de 89%) são números, sendo os números inteiros a maior fatia e representando cerca de 2/3 desses dados.

Análise de resultados

O volume de sinalização criada ilustra a sobrecarga gerada por cada um dos protocolos de transporte de informação de gestão. Quanto maior sobrecarga gerar o protocolo de comunicação, maior será o volume de sinalização criada para a mesma informação de gestão trocada. A sobrecarga criada determina a escalabilidade da interface na medida em que condiciona a quantidade de elementos gestores intermédios que podem ser geridos pelo gestor central.

A Figura 5.6 ilustra a variação do volume de sinalização com o crescimento do número de objectos de gestão trocados entre as entidades do cenário de testes.

A análise dos valores do volume de sinalização das mensagens trocadas entre as aplicações mostra uma grande diferença de desempenho entre as aplicações Diameter e WBEM. Enquanto a aplicação Diameter utilizou 2GB de informação, a aplicação WBEM atingiu aproximadamente os 12GB. Como se observa no gráfico da Figura 5.6, ambas as aplicações apresentam um crescimento linear do volume de sinalização com o aumento do número de objectos.

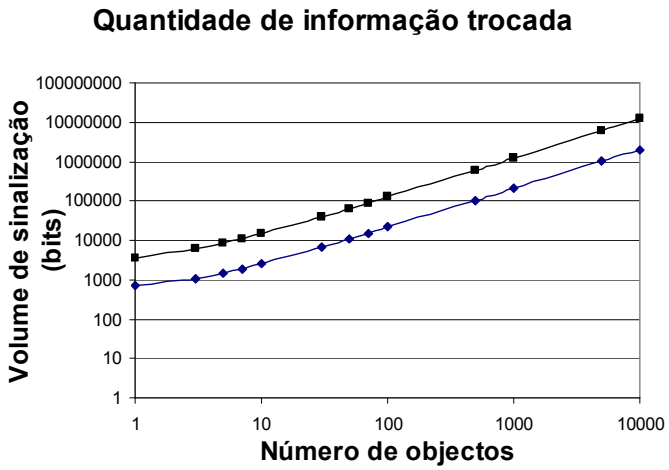

Figura 5.6 - Volume de sinalização das aplicações Diameter e WBEM.

Da análise dos requisitos de memória dos sistemas representados na Figura 5.7, pode-se verificar que a tendência de maior consumo de recursos da solução XML demonstrada em relação ao volume de sinalização se mantêm.

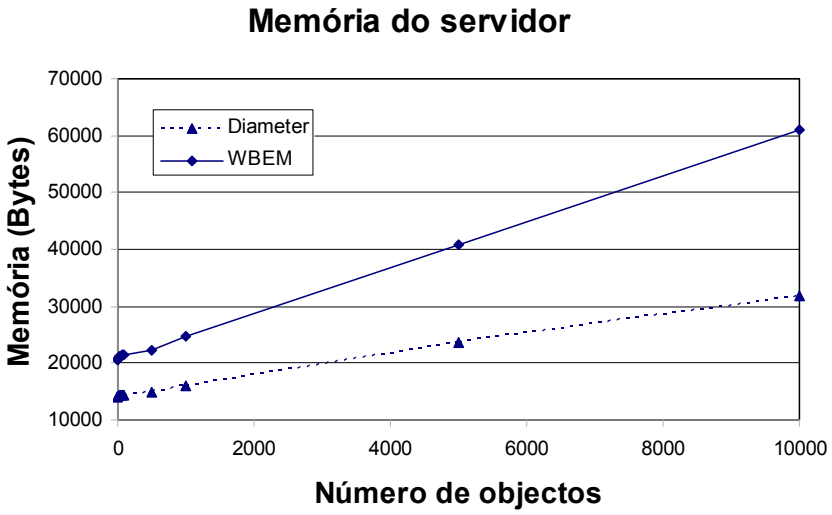

Figura 5.7 - Requisitos de memória.

Ambas as tecnologias mantêm um crescimento linear com o aumento do número de objectos, apresentando a tecnologia WBEM um crescimento mais elevado. Da análise do gráfico verifica-se ainda, através do valor das ordenadas na origem de ambas as rectas, que os requisitos de memória iniciais são diferentes. A explicação dessa diferença está relacionada com a diferença existente nas aplicações: enquanto que a aplicação Diameter foi especialmente desenvolvida para efectuar os testes, a aplicação de teste WBEM foi adaptada de um servidor WBEM [112],

mantendo um conjunto de funcionalidades originalmente presentes no servidor que não foram removidas.

Os valores de memória utilizados pelas aplicações atingiram para os 10000 objectos trocados cerca de 60 Kb no caso da implementação WBEM e pouco mais de 30KB no caso da aplicação Diameter, não apresentando qualquer das tecnologias algum problema de escalabilidade e permitindo uma fácil utilização num cenário de um operador.

Comparação com tecnologias alternativas

As alternativas consideradas para a implementação das interfaces foram o SNMP, COPS e Diameter, WBEM, *Web Services* e NETCONF: SNMP é o protocolo de gestão mais comum disponível na maioria dos equipamentos; COPS é um protocolo de gestão que na sua versão COPS-PR se adapta aos cenários de configuração de elementos e *Web Services* é uma tecnologia de desenvolvimento de sistemas distribuídas que ultimamente tem vindo a ser cada vez mais utilizado na área de sistemas de gestão.

Os valores de volume de sinalização obtidos, representados na Figura 5.8, confirmaram que: os protocolos binários apresentam um desempenho muito melhor do que os protocolos baseados em XML, que o mais eficiente dos protocolos é o COPS e que o protocolo que apresenta pior desempenho é o protocolo utilizado na tecnologia WBEM. Existem no entanto dois factos curiosos nos resultados dos testes: a diferença entre as prestações das tecnologias WBEM e WS; e a diferença entre os desempenhos dos protocolos binários, especialmente o protocolo SNMP.

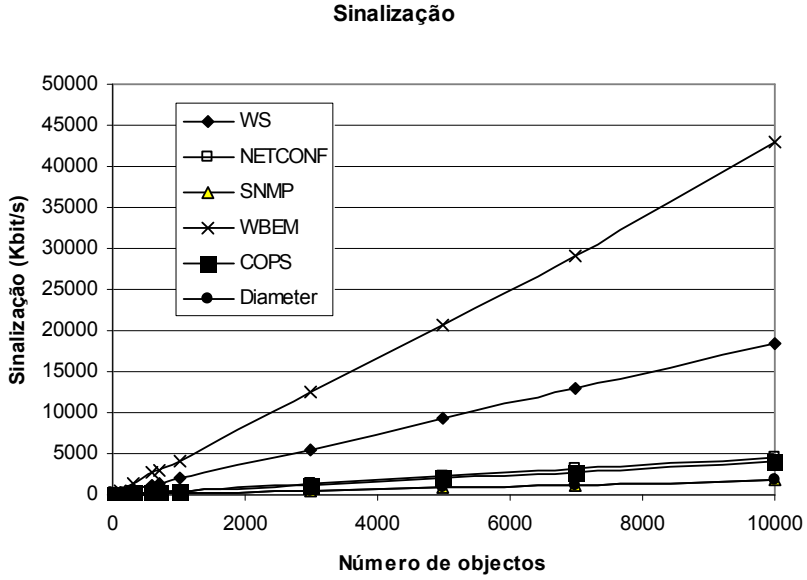

Figura 5.8 - Volume de sinalização.

A análise dos pacotes trocados na comunicação entre as entidades da tecnologia SNMP permitiu verificar que o desempenho foi comprometido, por um lado pelo carácter verboso do protocolo (especialmente devido ao formato dos *OIDs*), e por outro, pelo facto de as aplicações manterem um processo de sucessivos pedidos e respostas até que a transferência dos dados seja completa. As aplicações *COPS* e *Diameter*, pelo facto de utilizarem um protocolo de transporte com controlo de fluxo, limitam-se a colocar dentro da mesma mensagem o conjunto completo dos objectos que desejam transferir; as aplicações SNMP efectuam vários pedidos e respostas enviando a informação de uma forma segmentada, o que tem consequências em termos de tráfego gerado visto que os cabeçalhos dos pedidos e respostas influenciam a quantidade de tráfego gerado.

A análise dos pacotes trocados entre os elementos WBEM e *Web Services* permitiu verificar que apesar de ambos efectuarem uma codificação XML dos objectos, existia uma diferença entre a eficiência dos processos de codificação. A codificação de um objecto efectuada pelo servidor WBEM, ilustrada na Figura 5.9, utiliza um processo de codificação dos dados muito pouco eficiente, por três grandes razões. Em primeiro, porque descreve para cada uma das propriedades do objecto (o seu nome, o seu tipo e o seu valor) um extenso conjunto de valores, repetindo-os juntamente com as respectivas *tags* XML por cada um dos objectos trocados. A segunda razão tem a ver com o tamanho das *tags* XML utilizadas que, pelo menos quando comparados com o tamanho das *tags* XML utilizadas na tecnologia *Web Services*, é muito grande. A terceira razão tem a ver com a repetição completa da informação relativa à propriedade chave de cada objecto. Por cada objecto incluído na mensagem, o servidor WBEM descreve a propriedade chave do objecto identificando o seu valor, o nome e o tipo e depois repete toda essa informação, tal como faz em relação a qualquer outra propriedade do objecto.

```
<INSTANCENAME CLASSNAME="D_Interface"><KEYBINDING NAME="InterfaceID"> <KEYVALUE
VALUETYPE="numeric">39650</KEYVALUE></KEYBINDING></INSTANCE NAME></INSTANCEPATH><INSTANCE
CLASSNAME="D_Interface"><PROPERTY NAME="InterfaceID"
TYPE="uint16"><VALUE>39650</VALUE></PROPERTY><PROPERTY NAME="ADDR"
TYPE="string"><VALUE>2001:690:2380:778f:250:daff:fed6:499c</VALUE></PROPERTY><PROPERTY
NAME="Bandwidth"TYPE="uint16"><VALUE>10</VALUE></PROPERTY><PROPERTY NAME="Uplink"
TYPE="uint16"><VALUE>1</VALUE></PROPERTY><PROPERTY NAME="NetworkID"
TYPE="uint16"><VALUE>20064</VALUE></PROPERTY><PROPERTY NAME="Prefix"
TYPE="uint16"><VALUE>12</VALUE></PROPERTY><PROPERTY NAME="PrefADDR"
TYPE="string"><VALUE>214:748:364:217:222:2222:0001</VALUE></PROPERTY><PROPERTY
NAME="BWUnit" TYPE="uint16"><VALUE>2</VALUE></PROPERTY> <PROPERTY NAME="IfIndex"
TYPE="uint16"><VALUE>11</VALUE></PROPERTY></INSTANCE> </VALUE.OBJECTWITHPATH>
```

Figura 5.9 – Codificação de objecto WBEM.

No caso da tecnologia Web Services, os dados relativos à descrição dos campos dos atributos de um objecto são descritos através da definição do seu *schema*. Depois são definidos os valores de cada uma das propriedades de cada um dos objectos, sem que o seu tipo tenha que ser referido. Adicionalmente a definição das *tags*, como ilustrado na Figura 5.10, é efectuada de uma maneira muito mais racional, minimizando ao máximo a quantidade de informação inútil a ser

repetida em cada um dos objectos que compõe a mensagem. A codificação mais eficiente permite-lhe utilizar pouco mais de 40% do tráfego utilizado pela tecnologia WBEM.

```
<p:D_Interface xmlns:p=http://schemas.dmtf.org/wbem/wscim/1/cimschema/2/D_Interface
xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><p:InterfaceID>39639</p:InterfaceID><p
:ADDR>2001:690:2380:778f:250:daff:fed6:499c</p:ADDR><p:Bandwidth>10</p:Bandwidth><p:Uplink>
1</p:Uplink><p:NetworkID>20064</p:NetworkID><p:Prefix>12</p:Prefix><p:PrefADDR>214:748:364:
217:222:2222:0001</p:PrefADDR><p:BWUnit>1800</p:BWUnit><p:IfIndex>11</p:IfIndex></p:D_Inter
face>
```

Figura 5.10 – Codificação de objecto WS-Management.

A tecnologia NETCONF é das tecnologias baseadas em XML a que faz uma codificação mais eficiente. A mensagem de resposta NETCONF (Figura 5.11) inclui um pequeno envelope SOAP onde é definida a operação RPC e dentro deste é incluída a mensagem de resposta contendo a configuração codificada, também em XML.

```
<?xml version="1.0"?><rpc message-id="1"><get-config><source><running/></source><config>
<all/></config><format>xml</format></get-config></rpc><?xml version="1.0"?><!DOCTYPE
netconf.dtd><rpc-reply message-id="1"><config><D_Interface><InterfaceID>39649
</InterfaceID><ADDR>2001:690:2380:778f:250:daff:fed6:499c</ADDR><Bandwidth>10</Bandwidth><
Uplink>1</Uplink><NetworkID>20064</NetworkID><Prefix>12</Prefix><PrefADDR>214:748:364:217:2
22:2222:0001</PrefADDR><BWUnit>1800</BWUnit><IfIndex>11</IfIndex></D_Interface></config>
</rpc-reply>
```

Figura 5.11 – Mensagem de resposta completa NETCONF.

A eficiência de transporte de cada uma das tecnologias pode ser calculada através da relação entre a informação útil e a informação total trocada entre as aplicações envolvidas na comunicação. De acordo com os valores obtidos para cada uma das tecnologias e ilustrados na Figura 5.12, verifica-se que a eficiência de cada uma das tecnologias cresce com o crescimento do número de objectos. O aumento da eficiência deve-se à reutilização do mesmo cabeçalho para um maior número de objectos trocados. Verifica-se ainda que a eficiência máxima é obtida pelo protocolo COPS com cerca de 39%, logo seguido do protocolo Diameter com cerca de 12%.

A baixa eficiência das tecnologias baseadas em WBEM tem uma explicação óbvia que tem a ver com o carácter verboso do XML que se percebe pela observação da codificação dos objectos ilustrados na Figura 5.9 e na Figura 5.10. No caso do protocolo SNMP verifica-se que a sua eficiência cresce aproximadamente até aos 15 objectos, altura em que os objectos preenchem totalmente o pacote UDP, fixando-se no valor de aproximadamente 13%. Esse valor de eficiência não é ultrapassado porque a partir dele se repete o processo de pedido e resposta de novos objectos.

Em termos de tempo de resposta e de requisitos de memória das entidades envolvidas na comunicação os resultados seguem genericamente os obtidos para o volume de sinalização. A principal diferença encontrada tem a ver com a implementação Web Services que foi desenvolvida como um adaptador entre as tecnologias WBEM e WS-Management. Assim, e como explicado em

[113], pelo facto de o servidor Web Services efectuar a recodificação dos objectos, os valores de tempo de resposta e de memória utilizada são afectados.

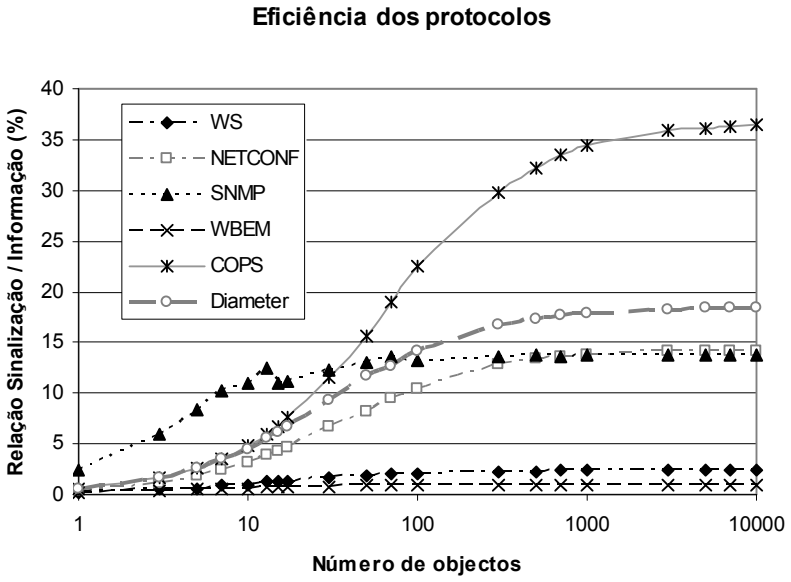

Figura 5.12 - Eficiência dos diferentes protocolos.

Com o objectivo de avaliar a utilidade das técnicas de compressão dos dados, foram desenvolvidos testes que consistiram na utilização de rotinas de compressão baseadas na biblioteca *zlib* sobre as mensagens trocadas entre as aplicações envolvidas no cenário. Os testes foram repetidos e os valores de volume de sinalização foram comparados com os valores do cenário anterior. A Figura 5.13 ilustra os resultados do ganho de compressão obtido no processo.

De uma forma geral, todas as tecnologias apresentaram um ganho de compressão, tendo cada uma delas um limite máximo diferente. Os ganhos de cada uma das tecnologias estão directamente relacionados com o carácter verboso de cada uma delas, sendo tanto maior quanto mais repetida for a informação presente na mensagem. Por exemplo o protocolo COPS é o protocolo com o crescimento do ganho mais lento. Tal como aconteceu nos testes anteriores, o protocolo SNMP não obteve um ganho considerável pelo facto de limitar a informação a incluir em cada mensagem. Tendo pouca informação; as rotinas de compressão não conseguem obter um ganho tão elevado como em mensagens com maior quantidade informação.

Os limites dos ganhos obtidos são extremamente elevados mostrando que, apesar de ser necessário contrabalançar o custo associado ao tempo de compressão, a técnica de compressão da informação poderá ser muito útil para cenários que envolvam grandes quantidades de informação.

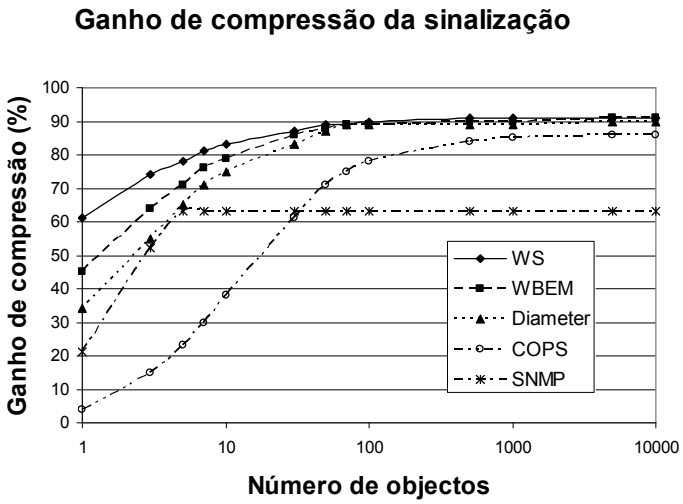

Figura 5.13 - Ganho de compressão da sinalização.

5.2.3 Desempenho da interface com elementos de rede

O desempenho da interface de comunicação entre os elementos gestores intermédios e os elementos de rede, ao contrário do desempenho da interface analisada na secção anterior, representa um elemento determinante no desempenho global de todo o sistema: a comunicação entre o gestor intermédio e os elementos de rede é muito frequente, visto que além de ocorrer durante os processos de configuração dos elementos de rede também se verifica no processo de admissão de novos fluxos.

Esta secção descreve testes de desempenho dessas interfaces, e apresenta os resultados obtidos. Também compara o seu desempenho com o obtido utilizando uma interface baseada no protocolo de comunicação COPS, tal como especificado na versão 6 da arquitectura NGN do 3GPP. Aqui são analisados os requisitos de largura de banda necessários ao transporte da sinalização, os requisitos de memória e o tempo de atraso no envio das mensagens.

Procedimento de teste das interfaces

Tendo em conta a especificação dos AVPs feita pelo 3GPP na especificação da interface *Gx* [77], foi desenvolvida uma interface de comunicação Diameter com vista à integração dos elementos de rede desenvolvidos no âmbito do projecto Daidalos com o elemento gestor intermédio. De entre as mensagens trocadas entre as entidades, as mais frequentes são as de *CC-Request* (CCR) cujo formato se encontra ilustrado na Figura 5.14, que representa um pedido de estabelecimento de um novo fluxo enviado pelo PCEF ao PCRF; e a mensagem *CC-Answer* (CCA)

que é enviada pelo PCRF ao PCEF respondendo ao pedido recebido. Da análise da estrutura das mensagens, tanto CCR como CCA, salienta-se a sua complexidade e dimensão.

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Destination-Host ]
                 [ Origin-State-Id ]
                 *[ Subscription-Id ]
                 [ Bearer-Control-Mode ]
                 [ Network-Request-Support ]
                 [ Bearer-Identifier ]
                 [ Bearer-Operation ]
                 [ Framed-IP-Address ]
                 [ Framed-IPv6-Prefix ]
                 [ IP-CAN-Type ]
                 [ RAT-Type ]
                 [ QoS-Information ]
                 [ QoS-Negotiation ]
                 [ QoS-Upgrade ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ 3GPP-SGSN-IPv6-Address ]
                 [ RAI ]
                 [ Bearer-Usage ]
                 [ Online ]
                 [ Offline ]
                 *[ TFT-Packet-Filter-Information ]
                 *[ Charging-Rule-Report]
                 *[ Event-Trigger]
                 [ Access-Network-Charging-Address ]
                 *[ Access-Network-Charging-Identifier-Gx ]
```

Figura 5.14 – Formato da mensagem CCR.

Segundo a especificação de arquitectura NGN feita pelo 3GPP, os pedidos de admissão de novos fluxos podem ainda ser efectuados ao PCRF pelo AF, numa interface designada de *Rx* [79], caso se trate de fluxos de dados estabelecidos através de um pedido ao P-CSCF [114]. Tal acontece na totalidade dos serviços multimédia disponibilizados pela rede NGN, o que representa a maioria dos pedidos efectuados ao PCRF. Apesar de a AF ser uma entidade que não está directamente relacionada com QdS, foi decidido implementar um protótipo da interface *Rx* e criar uma pequena aplicação de teste que foi utilizada para testar o desempenho da interface. Entre as mensagens implementadas na interface *Rx* as relacionadas com pedidos de controlo de admissão estão a *Re-Auth-Request* (RAR) enviada pelo AF ao PCRF e a *Re-Auth-Answer* (RAA) enviada pelo PCRF ao AF, tal como descrito em 2.3.6.

As aplicações foram colocadas no demonstrador do projecto e foi efectuada a captura dos pacotes do tráfego trocado entre ambas, durante os processos de admissão de recursos relativos a estabelecimento de novas reservas de fluxos.

Análise de resultados

Da análise do tamanho das mensagens verifica-se que as mensagens de CCR apresentam um tamanho médio de 810 bytes e que as mensagens de CCA apresentam um tamanho médio de 694 bytes. A Tabela 5.5 apresenta os valores dos tamanhos das mensagens trocadas entre entidades envolvidas em processos de controlo de admissão. No caso das mensagens trocadas através das interfaces *Gx,* verifica-se que apresentam tamanhos médios de 516 bytes para a mensagem RAR e 430 bytes para a mensagem RAA, perfazendo a comunicação completa um total de 946 bytes.

Tabela 5.5 - Resultados da medição das mensagens trocadas nas interfaces Rx e Gx.

INTERFACE	MENSAGEM	TAMANHO (BYTES)	TOTAL (BYTES)
Rx	RAR	516	946
	RAA	430	
Gx	CCR	810	1504
	CCA	694	

Contudo, analisando a estrutura da mensagem ilustrada na Figura 5.14, verifica-se que o seu conteúdo vai bastante além da informação necessária à tomada de decisão de admissão do novo recurso e que existe uma forte componente de informação relacionada com o registo de utilização. A comparação directa dos tamanhos das mensagens trocadas não pode assim ser feita, visto que as funcionalidades de ambas são diferentes e assim o resultado da comparação não seria justo.

Em [115] Gonçalves et al é descrito um processo de avaliação das tecnologias mais utilizadas nas interfaces especificadas nas propostas de arquitectura NGN do 3GPP nas versões 6 e 7 [115, 116]. No processo de avaliação é comparada a informação relativa ao desempenho das interfaces pertencentes a ambas as tecnologias, com os resultados de desempenho de outras duas plataformas desenvolvidas no projecto Daidalos [117] onde foram utilizados interfaces *COPS* e *Diameter*. Como a interface *Diameter* do projecto Daidalos se limita a transportar informação relativa ao processo de admissão, e dado que os interfaces COPS do interface *Go* e do projecto Daidalos apresentam desempenhos muito semelhantes, era estimada a componente de informação incluída nas mensagens CCR e CCA que estava relacionada com gestão de QdS, representando aproximadamente 712 bytes. A restante parcela representa informação relacionada com o registo de utilização. Comparando o tamanho das diversas mensagens das várias interfaces testadas, verificou-se que o tamanho das mensagens trocadas pela interface Diameter é aproximadamente o triplo do tamanho das mensagens trocadas por uma interface COPS equivalente.

5.3 Dimensionamento e análise de escalabilidade da solução

O cenário de teste descrito nesta secção, é definido com dois propósitos: em primeiro lugar dimensionar as entidades e os respectivos sistemas computacionais, e em segundo verificar a escalabilidade de cada elemento da solução de gestão.

Tendo em conta que tanto os dados respeitantes à dimensão das redes actuais dos operadores, como os estudos de dimensionamento de redes de operadores futuras não são acessíveis, o nosso estudo é desenhado com os seguintes pressupostos:

- corresponde a um hipotético operador de rede NGN, onde a convergência entre as redes fixa e móvel ocorreu;
- as infra-estruturas de rede e de controlo integram todas as redes de acesso;
- o operador actua à escala de um país com uma dimensão semelhante à de Portugal;
- a rede descrita no cenário é dimensionada de forma a funcionar nas horas de maior utilização.

Adicionalmente é assumido que o número de clientes corresponde à soma do número de clientes das diversas empresas que compõem o grupo nacional de telecomunicações com maior dimensão (Portugal Telecom), segundo números dos relatórios estatísticos publicados pela ANACOM relativos ao segundo trimestre de 2008. É ainda assumido que os diversos pontos de acesso às redes sem fios cobrem a área do território nacional, existindo em média um ponto de acesso por cada 4 Km^2.

A Tabela 5.6 lista o conjunto de características e de valores utilizados na elaboração do cenário, e posteriormente utilizado no processo de dimensionamento dos diversos elementos.

Tabela 5.6 - Descrição do cenário de análise.

QUANTIDADE	DESCRIÇÃO	COMENTÁRIO
1:15	Taxa de retenção	1:20 no ADSL sem compromissos de QdS
¼ Km^2	Gateways	
13200000	Utilizadores	Total do Universo PT
3	Serviços utilizados em simultâneo por utilizador	
90%	Percentagem dos utilizadores registrados em simultâneo na rede	
10%	Percentagem de clientes que se encontram simultaneamente a utilizar a rede, nas horas de maior utilização	
100000 Km^2	Área similar à área de Portugal	

Tendo em conta que a área considerada é aproximadamente de 100 000 Km^2, obtém-se um total de 25 000 pontos de acesso (*gateways*) às redes sem fios através da fórmula (1).

$$Total_{gateways} = \frac{100000Km^2}{\frac{4Km^2}{ponto \quad de \quad acesso}} = 25000 \qquad (1)$$

O número de elementos gestores de recursos é determinado por questões de desempenho da rede, sendo aumentado até ao desempenho ser adequado. De entre os factores cruciais na determinação do número de gestores de recursos, destacam-se a quantidade de pedidos de reservas e a quantidade de memória que o gestor necessita para armazenar a informação que descreve a sua rede e as reservas que aceitou.

De acordo com as condições do cenário, nas horas de maior utilização a infra-estrutura de rede receberá um número de pedidos de reserva que pode ser calculado através da expressão (2).

$$Num_{Ped}/_{seg} = \frac{13{,}2M \times 10\% \times 3}{30seg} = 132000\ ped/_{seg} \qquad (2)$$

Tendo em conta que o tamanho das mensagens RAR e RAA da interface Gx são respectivamente 810 e 694 bytes, cada um dos pedidos de reserva origina aproximadamente 1504 bytes. Assim o total de sinalização gerado pelos processos de pedido de reserva pode ser obtido por (3).

$$TotalSinalização = 132000 \times 1504 \times 8 \approx \frac{1515Mbit}{seg} \qquad (3)$$

Se o elemento gestor utilizar interfaces de rede *GigabitEthernet*, e de forma a evitar que as interfaces transportem mais do que 60% do seu limite físico, recomenda-se assim usar 3 elementos gestores para o volume de pedidos previstos.

Cada um dos pedidos aceites obriga o elemento gestor a reservar recursos da rede para o servir e a armazenar informação acerca das reservas aceites. Assim pode calcular-se o número total de reservas aceites pela rede através de (4).

$$Total_{\mathrm{Re}\,servas} = 13{,}2M \times 10\% \times 3 = 3960000 \qquad (4)$$

Atendendo a que a reserva deve conter informação acerca dos endereços de origem e de destino, os códigos DSCP e a largura de banda para ambos os fluxos, a estrutura de cada reserva deve ser semelhante à descrita na Tabela 5.7, perfazendo um tamanho total de 18 bytes.

Tabela 5.7 - Informação presente nas reservas.

COMPONENTE	TAMANHO(BYTE)
IP origem	4
IP destino	4
DSCP Uplink	1
DSCP Downlink	1
BW Uplink	4
BW downlink	4
Total	18

A quantidade de reservas aceites ocupa aproximadamente 68 Mb de memória ao sistema de gestão de recursos, o que não constitui qualquer tipo de sobrecarga para os três gestores anteriormente determinados.

Tal como em relação aos elementos gestores, os elementos de rede também deverão ser dimensionados de forma a garantir o desempenho global da rede. Os factores que mais limitam esse desempenho relacionam-se com o tráfego produzido no sentido da rede de core, e com a quantidade de memória necessária para armazenar as reservas dos recursos aceites pelo sistema gestor. Considerando que um elemento de rede possui uma interface com a rede de core com a largura de banda de 1Gb, que é disponibilizado aos clientes um serviço de 12 Mbitps e que a rede implementará uma taxa de retenção de 1:15, o número de clientes por elemento de rede pode ser obtido pela expressão em (5).

$$\frac{Clientes}{Elm\,\mathrm{Re}\,de} = \frac{1Gb}{\frac{12Mb}{15}} = 1280 \qquad (5)$$

Assim sendo, o número de elementos de rede necessários para a rede do cenário poderia ser determinado pela expressão (6).

$$Num_{Elementos} = \frac{13{,}2M \times 10\%}{1280} \approx 1032 \qquad (6)$$

De forma a poder efectuar a gestão dos pontos de acesso à rede os seus interfaces também devem ser descritos no sistema de gestão da rede. A Tabela 5.8 resume a quantidade necessária de cada um dos elementos que compõem o cenário de gestão.

Tabela 5.8 - Dimensão do cenário.

ELEMENTO	QUANTIDADE	COMENTÁRIO
Gestor de recursos	3	Determinado pelo volume de sinalização
Elementos de rede	1032	1 por cada 1280 clientes
Interface	27064	Soma das interfaces dos elementos de rede com as interfaces das gateways.
Pontos de acesso	25000	Um para cada 4Km^2

5.3.1 Dimensionamento e escalabilidade do gestor central

O gestor central do sistema armazena a informação de configuração de toda a rede, incluindo a lista de elementos das camadas inferiores e a sua descrição. Efectua a configuração dos elementos gestores intermédios definindo-lhes todos os detalhes relevantes acerca dos elementos da rede dos quais são responsáveis.

Atendendo ao carácter pouco dinâmico da intervenção do gestor central e ao facto de a configuração dos elementos gestores intermédios se efectuar antes da rede estar em funcionamento,

o tempo de resposta do gestor e o volume de sinalização trocado entre os gestores intermédios não são significativos. É no entanto significativo o efeito que a quantidade de informação tem sobre os requisitos de memória do gestor central.

A maior parcela de informação que o servidor central de gestão gere está relacionada com a descrição dos recursos da rede que gere. O servidor armazena informação acerca dos gestores intermédios, dos elementos de rede, das interfaces dos elementos de rede e dos pontos de acesso à rede sem fios. A Tabela 5.9 lista a quantidade de elementos de cada um dos grupos enumerados, bem como o tamanho de cada um dos elementos.

Tabela 5.9 – Dimensão da informação de configuração na memória do gestor central.

ELEMENTO	TAMANHO (BYTE)	QUANTIDADE	TOTAL (BYTE)
Gestor de recursos	68	3	204
Elementos de rede	44	1032	45408
Interface	22	27064	595408
Ponto de acesso	28	25000	700000
Total			1341020

De acordo com o cenário de gestão anteriormente descrito, o servidor central necessita de aproximadamente 1,3 MByte de memória para armazenar a informação que descreve os recursos da rede, valor que se pode considerar perfeitamente aceitável para uma sistema computacional actual. Acresce ainda que existe a opção de não armazenar a totalidade da informação na memória do sistema, libertando essa informação assim que o processo de configuração de gestores intermédios seja concluído. Nesse caso a informação mantida em memória limitar-se-ia à lista de gestores intermédios, sem que a degradação do tempo de resposta dos gestores intermédios pudesse ser um factor relevante por razões anteriormente descritas.

Depreende-se assim que a escalabilidade do gestor central não é um factor limitador da arquitectura proposta, podendo a solução ser aplicada a uma rede consideravelmente maior sem que sejam relevantes os efeitos a este nível.

5.3.2 Dimensionamento e escalabilidade do gestor intermédio

O gestor intermédio efectua o controlo de admissão de novas reservas e gere os recursos da rede de que é responsável. Mantém informação da rede que gere acerca dos elementos de rede, respectivas interfaces e dos pontos de acesso à rede sem fios. Recebe, avalia e responde a todos os pedidos de recurso da sua rede. Atendendo ao facto anteriormente mencionado de que a sua principal limitação se relaciona com a memória necessária para o armazenamento das reservas, e de ter sido anteriormente dimensionado durante o processo de dimensionamento do gestor central, o

presente dimensionamento é efectuado somente com o objectivo de determinar os requisitos computacionais do sistema que o possa instanciar.

Tendo em conta a subdivisão da rede, efectuada pelos vários elementos gestores intermédios, cada gestor necessita de manter somente a informação que descreve a parte da rede pela qual é responsável. Adicionalmente armazena informação acerca dos restantes elementos gestores intermédios para efeitos de estabelecimento de comunicação com eles. A Tabela 5.10 enumera os elementos presentes na memória do gestor intermédio, bem como o tamanho de cada um dos elementos.

Tabela 5.10 - Informação de configuração na memória do gestor intermédio.

ELEMENTO	TAMANHO (BYTE)	QUANTIDADE	TOTAL (BYTE)
Gestor de recursos	68	2	136
Elementos de rede	44	344	15136
Interface	22	9022	198484
Ponto de acesso	28	8334	233352
Total			447108

O número de elementos gestores intermédios, tal como descrito anteriormente, foi determinado de forma a suportar o armazenamento das reservas dos recursos pedidos pelos terminais. Tal como se pode observar através dos dados da Tabela 5.10 a informação referente aos elementos da rede de que é responsável não é de forma nenhuma um factor limitador da escalabilidade. De uma forma global, para aumentar a escalabilidade da camada de gestores intermédios deve subdividir-se a rede, instanciando um maior número de elementos gestores desta camada.

5.3.3 Dimensionamento e escalabilidade do elemento de rede

O dimensionamento dos elementos de rede inicialmente efectuado teve como objectivo garantir que a interligação com a rede de core fosse suficiente para transportar o tráfego gerado pela rede servida por cada um dos elementos. É ainda necessário verificar se a informação de gestão armazenada no elemento de rede e se a informação relativa às reservas servidas por esse elemento de rede não serão factores limitadores para o funcionamento do respectivo elemento.

Tendo em conta a segmentação da rede descrita anteriormente, a informação de gestão mantida na memória do elemento de rede limita-se à descrição do seu elemento gestor intermédio e às interfaces dos pontos de acesso presentes no segmento de rede que serve. A Tabela 5.11 lista os elementos de configuração presentes em cada um dos elementos de rede, que totalizam aproximadamente 1 Kbyte de informação.

Tabela 5.11 - Informação de configuração na memória do elemento de rede.

ELEMENTO	TAMANHO (BYTE)	QUANTIDADE	TOTAL (BYTE)
PCRF	68	1	68
Interface	22	27	594
Ponto de acesso	28	25	700
Total			1362

Assumindo que os 3,96 milhões de reservas simultaneamente aceites pela rede se distribuam uniformemente pelos 1032 elementos de rede, cada um dos elementos de rede deverá manter em memória aproximadamente 3838 reservas de recursos. Tendo em conta que cada reserva ocupará 18 bytes, cada elemento de rede ocupará aproximadamente 68 KByte de memória com essas mesmas reservas.

Tendo em conta ambas as quantidades de memória pode considerar-se que não serão factor determinante para o funcionamento do elemento de rede, podendo ser inclusivamente implementado por um equipamento actualmente utilizado pelos operadores, como por exemplo o Cisco CSE 1000.

5.3.4 Escalabilidade da interface com elementos de rede

A interface com os elementos de rede troca todas as mensagens associadas ao controlo de admissão de novos fluxos, podendo ser um motivo de limitação da escalabilidade da rede. A presente secção analisa a escalabilidade desta interface. Tendo em conta o processo de segmentação da rede anteriormente descrito, o crescimento do número de clientes não terá qualquer efeito no funcionamento da presente interface. O aumento do número de clientes teria como consequência um aumento dos elementos de rede e dos elementos gestores intermédios instanciados, pelo que o volume de sinalização trocado em cada um dos elementos se manteria constante. No entanto o que afectaria a sinalização trocada na interface, seria um aumento da taxa de simultaneidade de utilização dos elementos de rede, bem como uma diminuição do tempo de validade das reservas aceites.

A presente secção efectua uma análise do comportamento da interface com os elementos de rede, variando a taxa de utilização e o período de validade das reservas aceites pela rede. Os restantes parâmetros de funcionamento da rede mantêm-se tal como dimensionados nas secções anteriores.

A variação da simultaneidade de utilização da rede tem como efeito um aumento do número de clientes a utilizar os recursos da rede, efectuando consequentemente um maior número de pedidos de reserva e aumentando o volume de sinalização trocado entre os elementos gestores e os elementos de rede que gerem. Neste estudo foram analisados valores de simultaneidade entre 5 e

50% do total dos utilizadores servidos pelos elementos de rede geridos por cada um dos elementos gestores. A Figura 5.15 ilustra o efeito criado no volume de sinalização.

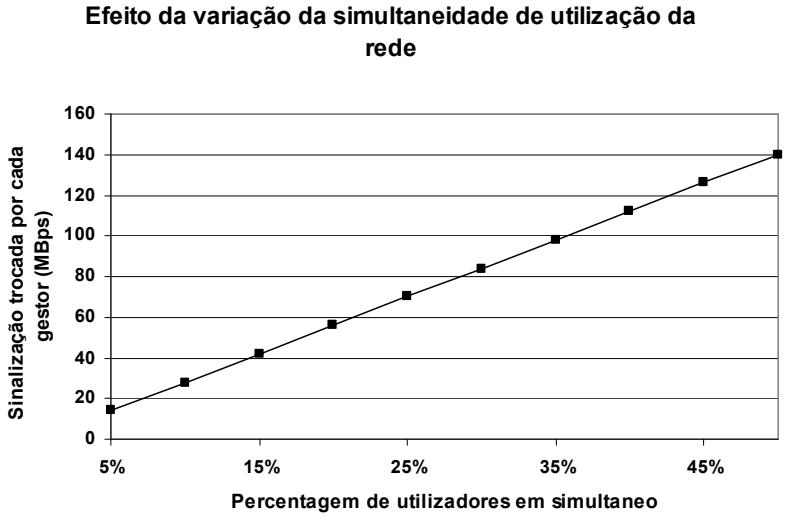

Figura 5.15 - Efeito da variação da simultaneidade de utilização da rede.

O volume de sinalização tem um crescimento linear, atingindo um valor máximo de aproximadamente 140 Mbps para o máximo de utilizadores de 50%. Este valor de sinalização pode ser considerado aceitável para a interface, que poderia ser implementada fisicamente por uma interface *gigabit ethernet*, e especialmente porque também corresponderia a um volume de tráfego de rede gerado pelos utilizadores que ultrapassaria o limite das interfaces de ligação dos elementos de rede à rede de core.

A variação do período de validade das reservas tem como consequência a troca de mensagens de renovação das mesmas, aumentando o número de mensagens trocadas por segundo e consequentemente aumentando o volume de sinalização trocado.

A Figura 5.16 ilustra a variação do volume de sinalização entre os elementos de rede e o elemento gestor para vários valores de validade das reservas.

O valor máximo de sinalização trocado atinge os 170 Mbps para períodos de validade de reserva de 5 segundos, o que constitui um valor perfeitamente aceitável para a capacidade da interface, permitindo diminuir ainda mais os períodos de reserva e implementar controlo de recursos com uma granularidade temporal de um segundo.

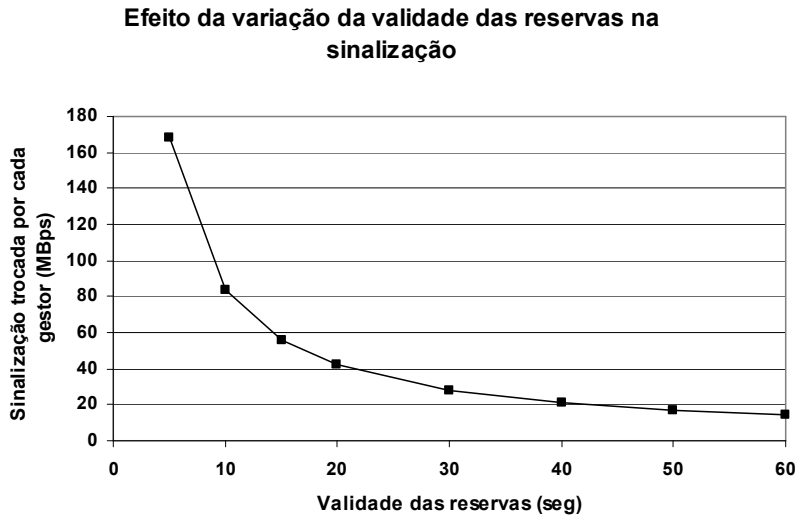

Figura 5.16 - Efeito da validade das reservas na sinalização trocada.

5.4 Conclusões

Nesta secção foi efectuada a análise da solução de gestão desenvolvida, do desempenho do servidor de politicas em termos de tempo de resposta e de sinalização gerada, bem como foram medidos os requisitos de memória do servidor. Verificou-se que, tanto a memória necessária, como os tempos de resposta do servidor não constituem qualquer problema ao desempenho da aplicação.

A análise da sinalização criada durante o processo de gestão mostrou que esta cresce linearmente com o aumento da informação de gestão. Apesar de o servidor conter a informação de gestão relativa a toda a rede do operador, não é no entanto factor limitativo à implementação da solução de gestão, uma vez que a transferência desta informação não é efectuada em tempo real, mas sim durante o processo de arranque das entidades da rede. Por outro lado, as actualizações desta informação serão efectuadas parcialmente e não muito frequentemente.

Para além disso, visto que a solução implementa adaptação do protocolo de comunicação, as interfaces comunicam através do protocolo NETCONF que gera um menor volume de sinalização do que a tecnologia WBEM do sistema de gestão central.

A análise de desempenho da interface com gestores intermédios determinou que apesar do elevado volume de sinalização produzido pelo protocolo NETCONF, a tecnologia escolhida é perfeitamente adequada para o desenvolvimento da interface em questão.

A comparação do protocolo NETCONF com protocolos de gestão alternativos demonstrou que o protocolo NETCONF é bastante eficiente, pelo menos comparado com outras tecnologias de gestão baseadas em XML. Na comparação verificou-se que os protocolos COPS e Diameter

apresentam uma menor sobrecarga de informação. O protocolo COPS tem a desvantagem de ser uma tecnologia abandonada, quer pela indústria quer pelos meios académicos, sem nunca ter conseguido implantar-se no mercado de gestão. O protocolo Diameter, apesar de ter forte implantação e muito especialmente nas redes NGN, apresenta uma sobrecarga computacional considerável devido à sua complexidade.

Durante a análise de desempenho dos protocolos da interface com elementos de rede, foram consideradas as tecnologias de gestão normalmente utilizadas nas propostas arquitecturais das redes NGN. Foi comparado o desempenho da interface *Go* pertencente à versão 6 da norma NGN do 3GPP com a interface *Gx* da versão 7. Verificou-se existir uma muito considerável diferença de desempenho das interfaces. Atendendo a que existe uma diferença de funcionalidade entre as interfaces recorreu-se à comparação com uma interface Diameter desenvolvida no âmbito do projecto Daidalos que implementa funcionalidades semelhantes ao interface *Go* do 3GPP. Verificou-se que a diferença de funcionalidades causa sensivelmente 50% da sobrecarga, enquanto que a diferença de desempenho origina os restantes 50%.

A análise de escalabilidade da interface com elementos de rede mostrou que é perfeitamente viável a aplicação de uma interface baseada em Diameter no processo de controlo de admissão de novos recursos.

Foi definido um cenário de utilização de forma a permitir o dimensionamento da rede, tendo posteriormente sido definido o número de elementos gestores intermédios, o número de elementos de rede e de pontos de acesso. Foram também determinados os requisitos dos sistemas computacionais que implementariam cada um dos elementos do sistema de gestão, que se encontram listados na Tabela 5.12.

Tabela 5.12 - Lista de requisitos de hardware.

Requisito	*Elemento*	*Grandeza*	*Descrição*
RH.1	Consola de gestão	512 MByte RAM	Memória
RH.2			Processador
RH.3		100Mbitps	Interface de rede
RH.4	Gestor central	2 GByte de RAM	Memória
RH.5			Processador
RH.6		100Mbitps	Interface de rede
RH.7	Elemento gestor de QdS	2 GByte RAM	Memória
RH.8			Processador
RH.9		1 Mbitps	Interface de rede
RH.10	Elemento de rede	64 MByte de RAM	Memória
RH.11			Processador
RH.12		1 Mbitps	Interface de rede

Os requisitos computacionais necessários à instanciação de cada um dos elementos do cenário são facilmente preenchidos pelo hardware actualmente existente no mercado, não constituindo por isso uma condicionante à implementação da solução de gestão proposta.

6 Conclusões e trabalho futuro

6.1 Síntese das conclusões

A evolução das redes de comunicações verificada na última década caracteriza-se por uma integração das redes de comunicação de voz com as redes de transmissão de dados, utilizando o protocolo IP como protocolo de rede, numa estratégia designada de *all-IP*.

A integração do tráfego destes dois tipos de rede com características diferentes, tanto em termos de necessidades de recursos, como em termos do valor dos serviços, aumentou a necessidade de implantação de mecanismos de garantia de QdS como forma de garantir a viabilidade económica das empresas prestadoras de acesso à rede. Os recursos de rede são partilhados pelos pacotes dos fluxos dos diferentes serviços, que tendo requisitos diferentes, obrigam ao estabelecimento de mecanismos de prioritização de tráfego.

A utilização massiva da tecnologia IP nas redes de comunicações tem vindo também a facilitar o desenvolvimento de novos serviços, com características e requisitos de recursos de rede diferentes, de que são exemplo os serviços de distribuição de vídeo e áudio em directo, serviços de jogo em rede ou partilha de ficheiros em redes P2P. Têm vindo a ser normalizadas e integradas com a tecnologia IP várias tecnologias de rede de acesso, especialmente de redes sem fios que têm ganho considerável popularidade e utilização. Estas tecnologias possuem diferentes características, desde a capacidade de transporte, à arquitectura de QdS, levando à criação de equipamentos de interligação específicos para cada tecnologia.

Ao crescimento da heterogeneidade de equipamentos e dos serviços que utilizam a rede, soma-se o crescimento de popularidade desses serviços e o correspondente aumento do número de utilizadores: tanto o número de clientes de serviços celulares, como o número de clientes de serviços de transmissão de dados têm aumentado de uma forma muito significativa.

A prestação de garantia de QdS numa rede com tais características é uma tarefa complexa, obrigando à utilização de mecanismos de gestão automática, onde se possa confiar a um sistema de gestão a configuração coordenada de todos os aspectos relacionados com o funcionamento dos equipamentos. Acresce ainda que a configuração deve ser efectuada à escala da rede do operador o que, devido à quantidade de equipamentos existentes na rede de um operador de comunicações,

deverá ser efectuado por um sistema de gestão de forma a garantir a configuração coordenada de toda a rede, bem como evitar os erros associados à intervenção humana.

Têm vindo a ser desenvolvidos esforços consideráveis no sentido de normalizar tecnologias de gestão de rede e sistemas, tanto por parte do DMTF como por parte do IETF. Foram propostos novos paradigmas de gestão, novos modelos de dados, novos protocolos de gestão e até linguagens de definição de informação de gestão. As tecnologias propostas têm vindo a disponibilizar novos mecanismos de gestão, novas possibilidades, e maior interoperabilidade, mas tem vindo também a requerer maiores requisitos computacionais, quer dos sistemas de gestão, quer dos elementos geridos por estes. Tais requisitos podem comprometer quer o desempenho da rede, quer a sua escalabilidade. Ao nível do sistema central de gestão a sobrecarga causada pelas tecnologias de gestão traduz-se num maior tempo de resposta do sistema de gestão e numa menor escalabilidade da arquitectura de gestão e da própria rede. Ao nível dos elementos da rede a sobrecarga tem consequências ao nível da capacidade de resposta dos elementos da rede às solicitações oriundas da própria rede. Devido às limitações de capacidade de processamento e de memória dos elementos de rede, a sobrecarga causada pela tecnologia de gestão pode comprometer o desempenho da rede, levando por exemplo os *routers* a descartarem pacotes por falta de memória ou de tempo para processar os seus cabeçalhos.

As arquitecturas NGN têm vindo a ser desenvolvidas por várias organizações ligadas aos operadores de telecomunicações como são exemplos o ITU-T, o 3GPP, ou o TISPAN, com o objectivo de normalizar uma plataforma modular de fornecimento de serviços multimédia a clientes de redes móveis. A estrutura modular destas arquitecturas desagrega as plataformas de gestão dos serviços e de gestão de recursos de transporte. Apesar de apresentarem diferenças, especialmente no que toca à nomenclatura apresentada, todas as arquitecturas partilham a mesma filosofia base bem como um componente designado de IMS, desenvolvido no âmbito dos esforços de normalização da arquitectura de rede NGN do 3GPP.

No centro do IMS existe um elemento, ao qual os terminais requerem o estabelecimento das sessões dos seus utilizadores. Esse elemento designado de CSCF, decide da aceitação dos pedidos de uma sessão com base no perfil dos utilizadores, bem como na informação relativa à disponibilidade de recursos fornecida pela entidade gestora de recursos. Permite aos operadores de rede de comunicações controlar o acesso aos vários operadores de serviços, obrigando-os para isso a um registo na plataforma de disponibilização de serviços, sob pena de os pedidos de acesso aos seus serviços serem negados ou mesmo reencaminhados para outro operador de serviços concorrente. Este mecanismo de controlo torna a arquitectura NGN mais interessante para os operadores de comunicações, que têm nos últimos anos visto os seus serviços descer na cadeia de

valor, ao mesmo tempo que continuamente têm aparecido e prosperado empresas cuja área de negócio utiliza os recursos das suas redes para funcionar.

De um modo geral as propostas de arquitectura de rede NGN limitam-se a definir detalhes relativos ao funcionamento da rede, não tendo ainda sido efectuada a definição da arquitectura de gestão. No caso do 3GPP, por exemplo, foram levantados os requisitos da plataforma de gestão e foi definida uma arquitectura de gestão ainda muito vaga.

Neste trabalho foi proposta uma arquitectura hierárquica de gestão assente em três camadas, segundo o paradigma de gestão baseada em políticas. A solução de gestão proposta visa gerir aspectos de QdS numa rede NGN, utilizando para isso um gestor de rede central que actua como ponto único de contacto entre o sistema de gestão e o administrador humano. Este servidor central garante a gestão dos elementos gestores da camada intermédia, que por sua vez asseguram a gestão dos elementos de rede.

Foi desenvolvido um gestor baseado na tecnologia WBEM utilizando uma implementação de software aberto e foram efectuadas extensões ao modelo de dados CIM. Foram também desenvolvidos três adaptadores de forma a gerir os aspectos relacionados com os objectos CIM criados e a efectuar a monitorização do comportamento da rede. Para permitir ao administrador uma configuração mais amigável do sistema, foi desenvolvida uma interface gráfica que além da edição dos elementos de configuração do sistema, permite também efectuar a especificação de uma forma gráfica e assistida das políticas de gestão da rede.

De forma a escolher a tecnologia de gestão mais adequada a cada uma das interfaces dos elementos das diferentes camadas do sistema, foram desenvolvidos e testados protótipos de diversas tecnologias. Foi analisado o desempenho de cada tecnologia, tendo sido comparados os requisitos de cada tecnologia em termos de memória, da sinalização criada e tempos de resposta. Verificou-se que as tecnologias baseadas em XML criam uma sobrecarga de sinalização e de memória, e que necessitam de tempos de resposta maiores. Verificou-se ainda que as tecnologias binárias são consideravelmente mais eficientes, entre as quais se destaca a tecnologia COPS.

Foram caracterizadas as necessidades de volume de informação de gestão e a frequência com que essa informação seria trocada entre as entidades pertencentes às várias camadas do sistema de gestão, tendo sido analisado o efeito dessa troca nas interfaces de comunicação das diversas entidades.

No caso da interface entre o gestor central e os elementos gestores intermédios foram escolhidas duas tecnologias: para as acções de configuração do sistema e para a comunicação da informação relacionada com eventos foi utilizada a tecnologia NETCONF; para a distribuição de informação de políticas foi utilizada a tecnologia Diameter, replicando o mecanismo de

comunicação da plataforma PCC do IMS. No caso da interface que interliga os elementos de rede foi reutilizada a plataforma proposta no âmbito da arquitectura do PCC.

Foi criado um demonstrador do sistema de gestão recorrendo aos elementos desenvolvidos e a alguns elementos disponibilizados por terceiros, tendo assim sido possível testar a arquitectura proposta.

A análise de escalabilidade demonstrou que a solução proposta se adequa a um cenário de grandes dimensões como o de um operador de telecomunicações, tanto ao nível do servidor central de gestão, como ao nível das interfaces de comunicação.

No caso da interface superior, verificou-se que as tecnologias de gestão baseadas em XML causam uma sobrecarga considerável, quer ao nível da sinalização, quer ao nível de tempo de resposta, quer ainda em relação à memória necessária nas entidades de gestão. O efeito da sobrecarga é ampliado pela dimensão do cenário (*e.g.*, pela quantidade de elementos de rede, pelo número de interfaces de rede dos elementos) criando um volume impressionante de sinalização, tempos de resposta consideráveis e elevadas quantidades de memória necessária.

Atendendo a que as mensagens trocadas através das interfaces superiores estão essencialmente relacionadas com acções de configuração, com um caracter pouco frequente, e que podem ser efectuadas em momentos de pouca carga da rede, o volume de informação de sinalização e o tempo de resposta às acções de configuração torna-se pouco relevante. Pelo facto de a troca de informação efectuada por essas interfaces se efectuar entre elementos gestores, com recursos de memória satisfatórios, o efeito do aumento da quantidade de memória não é também relevante.

No caso dos interfaces com os elementos de rede o estudo de escalabilidade mostrou que, apesar de a tecnologia baseada em COPS ser significativamente mais eficiente do que a tecnologia Diameter, esta última solução adequa-se perfeitamente, quer em relação à memória necessária, quer aos tempos de resposta do sistema. Para além disso utilizando tecnologia Diameter reutiliza-se uma API de comunicação já existente nos elementos de rede e utilizada em toda a plataforma IMS, obtendo assim ganho no custo de desenvolvimento e manutenção do software necessário.

6.2 Perspectivas de trabalho futuro

O trabalho apresentado nesta dissertação, encontra-se vocacionado para a gestão de recursos numa rede de próxima geração. Nesse sentido foram desenvolvidos e reutilizados vários componentes na criação de um demonstrador.

Existem, no entanto, diversos tópicos de melhoria da solução apresentada, desde logo a extensão da própria plataforma de gestão aos restantes componentes da rede NGN, de que são exemplos a gestão de utilizadores e a gestão de serviços.

Não foram também consideradas na solução de gestão questões relacionadas com a atomicidade das acções de configuração. Na impossibilidade de configurar um dos elementos de rede, a plataforma de gestão configurará os restantes elementos do domínio. Passarão a existir elementos com uma configuração desigual entre os elementos da rede, com todas as consequências que daí podem advir. Poder-se-ia implementar um mecanismo de transacções nas acções de configuração, dotando-as de um caracter atómico e assim evitar a existência de diferentes configurações entre os elementos da rede.

A solução apresentada neste trabalho não possui suporte de detecção / resolução de conflitos entre políticas. A detecção e resolução estática deste tipo de conflitos evitaria que o administrador de rede pudesse por engano ou distracção definir novas políticas que colidam com as políticas previamente especificadas. Permitiria ainda evitar fenómenos de instabilidade da rede devidos a políticas com acções contraditórias alternadamente executadas pelo sistema de gestão.

7 Referências

[1] J. Strassner, *Policy-Based Network Management: Solutions for the Next Generation*: Morgan Kaufmann, 2003.

[2] R. Boutaba and I. Aib, "Policy Based Management: A Histotical Perspective," *Journal of Network and Systems Management,* vol. 15, pp. 447-480, Dec 2007 2007.

[3] G. Cox, J. Serrat, J. Strassner, J. Souza, x0E, d. Neuman, D. Raymer, S. Samudrala, B. Jennings, and K. Barrett, "An Enhanced Policy Model to Enable Autonomic Communications," in *Engineering of Autonomic and Autonomous Systems, 2008. EASE 2008. Fifth IEEE Workshop on*, 2008, pp. 184-193.

[4] M. Casassa Mont, A. Baldwin, and C. Goh, "POWER prototype: towards integrated policy-based management," in *Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP*, 2000, pp. 789-802.

[5] D. Nicodemos, D. Naranker, L. Emil, and S. Morris, "The Ponder Policy Specification Language," in *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*, Bristol, UK, 2001, pp. 18 - 38.

[6] D. Agrawal, S. Calo, L. Kang-Won, and J. Lobo, "Issues in Designing a Policy Language for Distributed Management of IT Infrastructures," in *Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on*, 2007, pp. 30-39.

[7] D. Nicodemos, D. Naranker, L. Emil, and S. Morris, "The Ponder Policy Specification Language," in *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*: Springer-Verlag, 2001.

[8] DMTF, "CIM Simplified Policy Language (CIM-SPL)," Version: 1.0.0a ed, 2007.

[9] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "RFC 1157 - Simple Network Management Protocol (SNMP)," 1990.

[10] S. Omari, R. Boutaba, and O. Cherkaoui, "Enterprise directory support for future SNMPv3 network management applications," in *Global Telecommunications Conference, 1999. GLOBECOM '99*, 1999, pp. 2010-2014 vol.3.

[11] M. Stevens, W. Weiss, H. Mahon, B. Moore, J. Strassner, G. Waters, A. Westerinen, and J. Wheeler, "Policy Framework - draft-ietf-policy-framework-00," September 1999.

[12] M. Stevens, W. Weiss, H. Mahon, B. Moore, J. Strassner, G. Waters, A. Westerinen, and J. Wheeler, "Policy Framework - draft-ietf-policy-framework-00.txt," 1999.

[13] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, "RFC 2748 - The COPS (Common Open Policy Service) Protocol," T. I. E. T. F. (IETF), Ed., 2000.

[14] K. H. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, R. Yavatkar, and A. Smith, "RFC 3084 - COPS Usage for Policy Provisioning (COPS-PR)," T. I. E. T. F. (IETF), Ed., 2001.

[15] B. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "RFC2205 - Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," 1997.

[16] R. Sahita, S. Hahn, K. H. Chan, and K. McCloghrie, "RFC3318 - Framework Policy Information Base."

[17] T. F. Franco, W. Q. Lima, G. Silvestrin, R. C. Pereira, M. J. B. Almeida, L. M. R. Tarouco, L. G. Granville, A. Beller, E. Jamhour, and M. Fonseca, "Substituting COPS-PR: an evaluation of NETCONF and SOAP for policy provisioning," in *Policies for Distributed Systems and Networks, 2006. Policy 2006. Seventh IEEE International Workshop on*, 2006, pp. 10 pp.-204.

[18] *"Web-Based Enterprise Management (WBEM) Initiative"*, http://www.dmtf.org/standards/wbem/, 2008-12-14.

[19] DMTF, "Common Information Model (CIM) Specification - Version 2.2," 1999.

[20] DMTF, "Specification for the Representation of CIM in XML," 2002.

[21] DMTF, "Specification for CIM operations over HTTP version 1.1," 2003.

[22] *"C++ CIM/WBEM Manageability Services Broker"*, http://www.openpegasus.com, 2006-04-05.
[23] *"OpenWBEM project"*, www.openwbem.org, 2006-04-05.
[24] *"SBLIM - Standards Based Linux Instrumentation for Manageability"*, http://www-124.ibm.com/sblim/index.html, 2005-02-16.
[25] *"Java™ Web Based Enterprise Management"*, http://wbemservices.sourceforge.net/, 2006-04-05.
[26] *"SNIA - Storage Networking Industry Association: CIM/WBEM"*, http://www.snia.org/tech_activities/SMI/cim/, 2006-04-05.
[27] *"WMI - Windows Management Instrumentation"*, http://www.microsoft.com/whdc/system/pnppwr/wmi/default.mspx, 07/08/2007.
[28] P. Goncalves, J. L. Oliveira, and R. L. Aguiar, "A WBEM based solution for a 4G network integrated management," in *Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - AICT2005*: IEEE Computer Society, 2005.
[29] S.-J. Lee, M.-J. Choi, S.-M. Yoo, J. W. Hong, H.-N. Cho, C.-W. Ahn, and S.-I. Jung, "Design of a WBEM-based Management System for Ubiquitous Computing Servers," DMTF, 2006.
[30] DMTF, "CIM Event Model White Paper - DSP0107," 2003, p. 28.
[31] *"CIM Query Language Specification - DSP0202"*, http://www.dmtf.org/standards/published_documents/DSP0202_1.0.0.pdf, 2007-08-13.
[32] *"Common Information Model (CIM)"*, http://www.dmtf.org/standards/cim/, 07/09/2007.
[33] DMTF, "CIM Policy Model White Paper - CIM Version 2.7," 2.7.0 ed, 2003.
[34] B. Moore, "RFC 3460 - Policy Core Information Model (PCIM) Extensions."
[35] M. Wahl, T. Howes, and S. Kille, "RFC2251 - Lightweight Directory Access Protocol (v3)," 1997.
[36] X. Zhang, J. L. Tesseron, D. Seret, and C. Remy, "X.500 Directory and OSI management," in *Global Telecommunications Conference, 1992. Conference Record., GLOBECOM '92. Communication for Global Users., IEEE*, 1992, pp. 1106-1110 vol.2.
[37] J. Strassner, "How Policy Empowers Business-Driven Device Management," in *3rd International Workshop on Policies for Distributed Systems and Networks (POLICY'02)*, Monterey, California, 2002.
[38] H. Tada, W. Usui, and W. Xu Jian, "An approach toward implementation of OSS/BSS using NGOSS," in *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003, pp. 57-59 vol.1.
[39] OMG, "Unified Modeling Language Specification," 2005.
[40] T. T. Forum, "Shared Information/Data (SID) Model, Business View Concepts, Principles, and Domains, Release 7.5," 2008.
[41] W. Vambenepe, "Web Services Distributed Management: Management Using Web Services (MUWS 1.0)," OASIS, Ed., 2005.
[42] OASIS, "eXtensible Access Control Markup Language 3 (XACML) Version 2.0," OASIS, Ed., 2005.
[43] DMTF, "Web Services for Management (WS-Management)," in *DSP0226*, 2005.
[44] I. Sedukhin, "Web Services Distributed Management: Management of Web Services (WSDM-MOWS) 1.0. ," OASIS, Ed., 2005.
[45] D. Booth and C. K. Liu, "Web Services Description Language (WSDL) Version 2.0 Part 0: Primer," W3C, Ed., 2007.
[46] G. Pavlou, P. Flegkas, S. Gouveris, and A. A. L. A. Liotta, "On management technologies and the potential of Web services," *Communications Magazine, IEEE,* vol. 42, pp. 58-66, 2004.
[47] DMTF, "WS-CIM Mapping Specification," in *DSP0230*, 2006.
[48] DMTF, "WS-Management — CIM Binding," in *DSP0227*, 2006.
[49] C. Rigney, A. C. Rubens, W. A. Simpson, and S. Willens, "RFC2865 - Remote Authentication Dial In User Service (RADIUS)," 2000.
[50] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "RFC 3588 - Diameter Base Protocol," 2003.
[51] M. A. Garcia-Martin, M.-C. Belinchon, M. A. Pallares-Lopez, C. Canales-Valenzuela, and K. Tammi, "RFC 4740 - Diameter Session Initiation Protocol (SIP) Application," 2006.
[52] V. Y. H. Kueh and M. Wilson, "Evolution of Policy Control and Charging (PCC) Architecture for 3GPP Evolved System Architecture," in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, 2006, pp. 259-263.

[53] H. Ji, Z. Bin, L. Guohui, G. Xuesong, and L. Yan, "Challenges to the New Network Management Protocol: NETCONF," in *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*, 2009, pp. 832-836.
[54] C. Huiyang, Z. Bin, L. Guohui, G. Xuesong, and L. Yan, "Contrast Analysis of NETCONF Modeling Languages: XML Schema, Relax NG and YANG," in *Communication Software and Networks, 2009. ICCSN '09. International Conference on*, 2009, pp. 322-326.
[55] X. Hui and X. Debao, "Data modeling for NETCONF-based network management: XML schema or YANG," in *Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on*, 2008, pp. 561-564.
[56] J. Schonwalder, "Protocol-Independent Data Modeling: Lessons Learned from the SMIng Project," *Communications Magazine, IEEE,* vol. 46, pp. 148-153, 2008.
[57] E. Ellesson, B. Moore, J. Strassner, and A. Westerinen, "RFC3060 - Policy Core Information Model," 2001.
[58] Y. Ramberg, Y. Snir, J. Strassner, R. Cohen, and B. Moore, "RFC 3644 - Policy Quality of Service (QoS) Information Model," 2003.
[59] J. Boyle, R. Cohen, D. Durham, R. Rajan, S. Herzog, and A. Sastry, "RFC 2749 - COPS usage for RSVP," T. I. E. T. F. (IETF), Ed., 2000.
[60] B. Moore, D. Durham, J. Strassner, A. Westerinen, and W. Weiss, "RFC3670 - Information Model for Describing Network Device QoS Datapath Mechanisms," 2004.
[61] A. Karnik and A. Kumar, "Performance analysis of the Bluetooth physical layer," in *Personal Wireless Communications, 2000 IEEE International Conference on*, 2000, pp. 70-74.
[62] J. Lansford, A. Stephens, and R. Nevo, "Wi-Fi (802.11b) and Bluetooth: enabling coexistence," *Network, IEEE,* vol. 15, pp. 20-27, 2001.
[63] I. Papapanagiotou, D. Toumpakaris, J. Lee, and M. Devetsikiotis, "A survey on next generation mobile WiMAX networks: objectives, features and technical challenges," *Communications Surveys & Tutorials, IEEE,* vol. 11, pp. 3-18, 2009.
[64] *"3GPP home page"*, http://www.3gpp.org/, 2008-02-29.
[65] *"TISPAN"*, http://www.etsi.org/tispan/, 2008-02-29.
[66] *"Broadband Forum"*, http://www.broadband-forum.org/, 2009-02-24.
[67] *"Open Mobile Alliance"*, http://www.openmobilealliance.org/, 2008-02-28.
[68] *"IPSphere Forum"*, http://www.ipsphereforum.org/, 2008-02-29.
[69] R. Christian Esteve and R. Andreas, "A Review of Policy-Based Resource and Admission Control Functions in Evolving Access and Next Generation Networks," *J. Netw. Syst. Manage.,* vol. 16, pp. 14-45, 2008.
[70] ITU-T, "General Principles and General Reference Model for the Next Generation Networks." vol. Rec. Y.2011, 2004.
[71] A. Liotta and L. Lin, "The Operator's Response to P2P Service Demand," *Communications Magazine, IEEE,* vol. 45, pp. 76-83, 2007.
[72] ITU-T, "Functional requirements and Architecture of the NGN." vol. Rec. Y.2012, 2004.
[73] S. Jongtae, C. Mi Young, L. Soon Seok, and J. Jinoo, "Overview of ITU-T NGN QoS Control," *Communications Magazine, IEEE,* vol. 45, pp. 116-123, 2007.
[74] 3GPP, "IP Multimedia Subsystem (IMS); Functional Architecture," Release 8 ed: 3GPP, 2007.
[75] 3GPP, "IP Multimedia Subsystem (IMS) Stage 2," Release 8 ed: 3GPP, 2008.
[76] 3GPP, "Universal Mobile Telecommunications System; Policy and charging architecture," Release 8 ed, 3GPP, Ed., 2008.
[77] 3GPP, "Policy and charging control over Gx reference point," 2008.
[78] A. Terzis, L. Wang, J. Ogawa, and L. Zhang, "A two-tier resource management model for the Internet," in *Global Telecommunications Conference, 1999. GLOBECOM '99*, 1999, pp. 1779-1791 vol.3.
[79] 3GPP, "Policy and charging control over Rx reference point," Release 8 ed, 2008.
[80] TISPAN, "NGN Functional Architecture," V2.0.0 ed. vol. ETSI ES 282 001, 2008.
[81] T. Kovacikova and P. Segec, "NGN Standards Activities in ETSI," in *Networking, 2007. ICN '07. Sixth International Conference on*, 2007, pp. 76-76.
[82] D. Forum, "Policy control framework for DSL," Working text WT-134 Rev. 2 ed, 2006.
[83] *"CableLabs Home"*, http://www.cablelabs.com/, 2009-12-15.
[84] 3GPP2, "All-IP Core Network Multimedia Domain," X.S0013-000-0 v2.0 ed, 2009.
[85] 3GPP2, "All-IP Core Network Multimedia Domain - IP Multimedia Subsystem – Stage 2," 3GPP2 X.S0013-002-0 ed, 2009.

[86] Y. Bernet, R. Yavatkar, P. Ford, F. Baker, L. Zhang, M. Speer, B. Braden, B. Davie, E. Felstaine, and J. Wroclawski, "RFC2998 - A Framework for Integrated Services Operation over Diffserv Networks," 2000.
[87] B. Braden, D. Clark, and S. Shenker, "RFC1633 - Integrated Services in the Internet Architecture: an Overview," 1994.
[88] S. Blake, D. L. Black, M. A. Carlson, E. Davies, Z. Wang, and W. Weiss, "RFC 2475 - An Architecture for Differentiated Services," 1998.
[89] D. Gomes, P. Gonçalves, and R. L. Aguiar, "A Transsignaling Strategy for QoS Support in Heterogeneous Networks," in *11th International Conference on Telecommunications - ICT 2004*, Fortaleza, Brasil, 2004, pp. 1114-1121.
[90] 3GPP, "Telecommunication management; Principles and high level requirements," Release 8 ed, 2007.
[91] 3GPP, "Telecommunication management; Architecture," Release 7 ed, 2008.
[92] R. Yavatkar, D. Pendarakis, and R. Guerin, "RFC 2753 - A Framework for Policy-Based Admission Control."
[93] 3GPP, "Telecommunication management; Fault Management; Part 1: 3G fault management requirements," Release 8 ed, 2009.
[94] 3GPP, "Telecommunication management;Configuration Management (CM);Concept and high-level requirements," Release 8 ed, 2009.
[95] R. Neisse, R. Vianna, L. Granville, M. Almeida, and L. Tarouco, "Implementation and bandwidth consumption evaluation of SNMP to Web services gateways," in *Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP*, 2004, pp. 715-728 Vol.1.
[96] S.-M. Yoo, H. T. Ju, and J. W. Hong, "Performance Improvement Methods for NETCONF-Based Configuration Management " in *Management of Convergence Networks and Services*: Springer Berlin / Heidelberg, 2006, pp. 242-252.
[97] R. C. Pereira and L. Z. Granville, "On the performance of COPS-PR and NETCONF in an integrated management environment for DiffServ-enabled networks," in *Telecommunications, 2008. ICT 2008. International Conference on*, 2008, pp. 1-6.
[98] W. Rui, Z. Bin, L. Guohui, L. Yan, and G. Xuesong, "The Implementation and Analysis of the Monitoring Module based on NETCONF," in *Information Science and Engieering, 2008. ISISE '08. International Symposium on*, 2008, pp. 12-15.
[99] *The Windows Interface Guidelines for Software Design: An Application Design Guide (Microsoft Corporation) (Paperback)*: Microsoft Corporation, 1995.
[100] *"Apache Imperius"*, http://incubator.apache.org/imperius/, 2008-02-12.
[101] P. Gonçalves, C. Figueira, R. Azevedo, R. Aguiar, and J. L. Oliveira, "A graphical user interface for policy composition in CIM-SPL," in *IEEE International Workshop on Management of Emerging Networks and Services - MENS 2009*, St.-Petersburg, Russia, 2009.
[102] *"Sun WBEM SDK"*, http://wbemservices.sourceforge.net/, 2009-04-05.
[103] *"YENCA"*, http://sourceforge.net/projects/yenca/, 2009-04-05.
[104] *"Shipnet - Service handling on IP networks"*, http://www.ptinovacao.pt/cms/source/pdf/8807e30af58c5175e3cfc098ca900381.pdf, 2009-12-15.
[105] M. Hutter, A. Szekely, and J. Wolkerstorfer, "Embedded system management using WBEM," in *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, 2009, pp. 390-397.
[106] S.-M. Yoo, J. W.-K. Hong, J.-G. Park, C.-W. Ahn, and S.-W. Kim, "Performance Evaluation of WBEM Implementations," *KNOM Review* vol. Vol. 8, No. 2, pp. 7-13, February 2006 2006.
[107] Y. Zeng, C. Hobbs, J. Bell, and B. Quirt, "WBEM Server Benchmarks," Erickson 2003.
[108] D. Gomes, "COPS++."
[109] *"Agent++ - SNMPv1/v2c/v3 Agent API for C++"*, http://www.agentpp.com/, 2008-06-09.
[110] J. Schönwälder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, "SNMP Traffic Analysis: Approaches, Tools, and First Results," in *Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on*, 2007, pp. 323-332.
[111] *"Openwsman | WS - Management for All"*, http://www.openwsman.org/, 02-05-2008.
[112] *"OpenWBEM source code repository"*, http://sourceforge.net/projects/openwbem/, 2006-04-05.
[113] P. Gonçalves, J. L. Oliveira, and R. L. Aguiar, "An evaluation of network management protocols," in *11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009)*, New York, USA, 2009.

[114] J. J. P. Balbas, S. Rommer, and J. Stenfelt, "Policy and charging control in the evolved packet system," *Communications Magazine, IEEE,* vol. 47, pp. 68-74, 2009.
[115] P. Gonçalves, R. Azevedo, D. Gomes, J. L. Oliveira, and R. L. Aguiar, "Evaluation of Policy Based Admission Control Mechanisms in NGN," in *International Conference on Telecommunications 2009*, Marrakech, Morocco, 2009.
[116] 3GPP, "Policy control over Go interface," Release 6 ed, 2005.
[117] R. Azevedo, A. Oliveira, F. Fontes, D. Guerra, P. Esteves, and T. Mota, "End-to-end QoS implementation in a B3G network," in *Advanced Industrial Conference on Telecommunications (AICT 2005)*, Lisbon, Portugal, 2005, pp. 122-127.

Anexos

8 Anexo A

Tabela 8.1 - Lista de comandos Diameter.

NOME DO COMANDO	ABREV.	CÓDIGO
AA-Request	AAR	265
AA-Answer	AAA	265
Diameter-EAP-Request	DER	268
Diameter-EAP-Answer	DEA	268
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Credit-Control-Request	CCR	272
Credit-Control-Answer	CCA	272
Capabilities-Exchange-Request	CER	257
Capabilities-Exchange-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275
User-Authorization-Request	UAR	300
User-Authorization-Answer	UAA	300
Server-Assignment-Request	SAR	301
Server-Assignment-Answer	SAA	301
Location-Info-Request	LIR	302
Location-Info-Answer	LIA	302
Multimedia-Auth-Request	MAR	303
Multimedia-Auth-Answer	MAA	303
Registration-Termination-Request	RTR	304
Registration-Termination-Answer	RTA	304
Push-Profile-Request	PPR	305
Push-Profile-Answer	PPA	305
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309
Bootstrapping-Info-Request	BIR	310
Bootstrapping-Info-Answer	BIA	310
Message-Process-Request	MPR	311
Policy-Data-Request	PDR	314
Policy-Data-Answer	PDA	314
Policy-Install-Request	PIR	315
Policy-Install-Answer	PIA	315

9 Anexo B – Lista de requisitos do sistema de gestão

Tabela 9.1 - Lista de requisitos funcionais do sistema de gestão 3GPP TS 32.102.

REQ	DESCRIÇÃO	COMPRIMENTO
Rf.1	Ser capaz de gerir equipamento de diferentes fabricantes.	Cumprido
Rf.2	Desenvolver mecanismos de automatização de forma a optimizar eficiência e efectividade.	Cumprido
Rf.3	Sistema de configuração deve ser suficientemente flexível que permita o rápido desenvolvimento de serviços.	Cumprido
Rf.4	Deve reportar eventos e acontecimentos em formato normalizado de forma a permitir controlo remoto.	Cumprido
Rf.5	Deve permitir interoperabilidade entre operador de rede e operadores de serviços para troca de informação de gestão e contabilização.	Parcialmente
Rf.6	Solução deve ser escalável e deve suportar redes de diferentes dimensões.	Cumprido
Rf.7	Sistema de gestão deve permitir acesso a informação de gestão.	Cumprido
Rf.8	Deve reutilizar standards das TI sempre que possível.	Cumprido
Rf.9	Deve minimizar a complexidade de gestão da rede.	Cumprido
Rf.10	Utilizar interfaces normalizadas para a comunicação entre os elementos de rede e elementos de gestão.	Cumprido
Rf.11	Deve minimizar os custos de gestão.	Não avaliado
Rf.12	Fornecer um sistema integrado de gestão de falhas.	Não cumprido
Rf.13	Suportar operações de manutenção remotas de forma a simplificar interacções de suporte.	Cumprido
Rf.14	Deve suportar gestão de segurança com ênfase particular em situações e roaming automático e em redes de troca de pacotes.	Não cumprido
Rf.15	Suportar mecanismos de facturação flexíveis de forma a se poderem aplicar entre redes de diferentes operadores.	Não aplicável
Rf.16	Suportar gestão e avaliação do desempenho.	Parcialmente
Rf.17	Centralizar informação para que a alteração de um parâmetro se repercuta em toda a rede à escala do domínio de gestão.	Cumprido
Rf.18	Deve incluir mecanismos de restauração do sistema, (*e.g.*. re- sincronização e utilização de transacções).	Parcialmente

Tabela 9.2 - Lista de requisitos funcionais do sistema de gestão.

REQ	DESCRIÇÃO	CUMPRIMENTO
Rf.19	Criação de recursos e elementos de rede	Cumprido
Rf.20	Apagar recursos e elementos de rede	Cumprido
Rf.21	Configurar recursos e elementos de rede	Cumprido
Rf.22	Remover recursos da rede não operacionais, se necessário, de forma a minimizar distúrbios de funcionamento	Cumprido
Rf.23	Desacoplar modificações físicas das modificações lógicas	Cumprido
Rf.24	Completar todas as acções de configuração antes de disponibilizar recurso de rede.	Cumprido
Rf.25	Interface de comunicação entre gestor central e elementos de gestão intermédia deve poder ser desligada	Cumprido
Rf.26	Informação deve poder ser enviada para o gestor central assim que produzida	Cumprido
Rf.27	Informação deve poder ser enviada para qualquer dos gestores centrais (um ou vários)	Não aplicável
Rf.28	Definição de limiares individuais para a geração de eventos	Não cumprido
Rf.29	Capacidade de ser transportado em toda a rede independentemente da tecnologia de rede em questão (linhas dedicadas, X.25, ATM, Frame Relay, ...)	Cumprido
Rf.30	Representar um custo baixo e ser fiável	Cumprido
Rf.31	Detectar analisar e reportar eventos de falha de recursos	Cumprido
Rf.32	Efectuar a análise da localização das falhas	Não cumprido
Rf.33	Corrigir falhas de recursos	Cumprido
Rf.34	Sistema de reporte de falhas deve fornecer informação a outros processos de gestão de problemas	Cumprido
Rf.35	Sistema de administração de falhas deve gerir e verificar actividades de reparação de falhas	Não cumprido
Rf.36	Verificar se recursos se encontram disponíveis	Cumprido
Rf.37	Alocar recursos correctamente os recursos necessários à disponibilização do serviços	Cumprido
Rf.38	Efectuar reserva prévia de recursos necessários para determinado período	Não cumprido
Rf.39	Configurar e activar apropriadamente recursos	Cumprido
Rf.40	Testar e garantir que recurso funciona adequadamente e respeita valores de desempenho adequados.	Cumprido
Rf.41	Actualiza inventário de recursos em repositório adequado	Cumprido
Rf.42	Deve permitir reconfigurar centralmente a indicador de severidade dos alarmes	Não cumprido
Rf.43	Permitir a salvaguarda da informação de gestão.	Parcialmente

Tabela 9.3 - Lista de requisitos de facilidade de utilização.

REQ	DESCRIÇÃO	CUMPRIMENTO
Rfu.1	Interface gráfica deve autenticar o administrador da rede junto ao CIMOM.	Cumprido
Rfu.2	Interface gráfica deve permitir acesso a todos os elementos de configuração do sistema.	Cumprido
Rfu.3	Interface gráfica deve permitir acesso a toda a informação de monitorização do sistema.	Não cumprido
Rfu.4	Interface de configuração deve permitir acesso a toda à lista de eventos do sistema.	Não cumprido
Rfu.5	Interface gráfica deve permitir a edição dos recursos da rede a gerir.	Cumprido
Rfu.6	Interface gráfica deve permitir ao administrador a visualização da lista de eventos.	Cumprido
Rfu.7	Interface gráfica deve permitir a edição dos serviços de rede.	Cumprido
Rfu.8	Interface gráfica deve permitir a edição dos serviços de A4C.	Não aplicável
Rfu.9	Interface gráfica deve permitir a edição das políticas de forma gráfica, incluindo as três componentes da política: evento, condição e acção.	Cumprido
Rfu.10	Permitir a edição de políticas utilizando uma linguagem de especificação.	Cumprido
Rfu.11	Permitir a exportação de políticas para outros sistemas de gestão.	Cumprido
Rfu.12	Permitir a importação de outros sistemas de gestão.	Cumprido
Rfu.13	Proteger o sistema de erros cometidos pelo administrador do sistema no processo de especificação de políticas	Cumprido
Rfu.14	Deve facilitar o processo de composição de políticas recorrendo a metáforas gráficas conhecidas.	Cumprido
Rfu.15	Deve auxiliar o administrador do sistema no processo de especificação de políticas minimizando dificuldades relativas ao conhecimento da sintaxe e da semântica das linguagens de especificação de políticas.	Cumprido

Tabela 9.4 - Lista de requisitos de desempenho.

REQ	DESCRIÇÃO	CUMPRIMENTO
Or.1	Sistema deve suportar rede com 40M de utilizadores.	Cumprido
Or.2	Deve suportar a utilização de pelo menos 3 serviços em simultâneo por utilizador.	Cumprido
Or.3	Sistema deve efectuar a configuração de 20000 PCEF.	Cumprido
Or.4	Sistema deve efectuar a configuração de 10 PCRF.	Cumprido
Or.5	Sistema deve efectuar a configuração de 80000 interfaces de rede.	Cumprido

Tabela 9.5 – Normas e regulamentação aplicáveis.

REQ	DESCRIÇÃO	CUMPRIMENTO
NA.1	Utilização de soluções normalizadas.	Cumprido
NA.2	Utilização de interfaces abertas.	Cumprido
NA.3	Utilização de modelos de dados abertos e capazes de integrar a informação de gestão de toda a rede.	Cumprido
NA.4	Utilização de protocolos IEEE.	Cumprido
NA.5	Utilizar linguagens de especificação de políticas abertas e normalizadas	Cumprido

Tabela 9.6 – Outros requisitos não funcionais.

REQ	DESCRIÇÃO	CUMPRIMENTO
Or.1	Deve ser flexível, permitindo especificar novas políticas não previstas durante a análise de requisitos.	Cumprido
Or.2	Deve ser modular, permitindo instanciar novos elementos de gestão, aumentando assim a escalabilidade global	Cumprido
Or.3	Deve ser autónoma permitindo a gestão dos equipamentos de acordo com as políticas definidas sem mais intervenção do operador humano.	Cumprido
Or.4	Deve ser robusta de forma a suportar falhas de comunicação entre elementos do cenário.	Cumprido
Or.5	Deve ser escalável permitindo gerir redes de operador de pequena, média ou grande dimensão.	Cumprido
Or.6	Deve recuperar a falhas, especialmente a falhas de comunicação entre elementos do sistema de gestão.	Cumprido
Or.7	Deve poder ser facilmente integrada com sistemas empresariais do operador de forma permitir a integração entre sistemas de gestão da rede e gestão do negócio	Cumprido

10 Anexo C – Modelos de dados completos

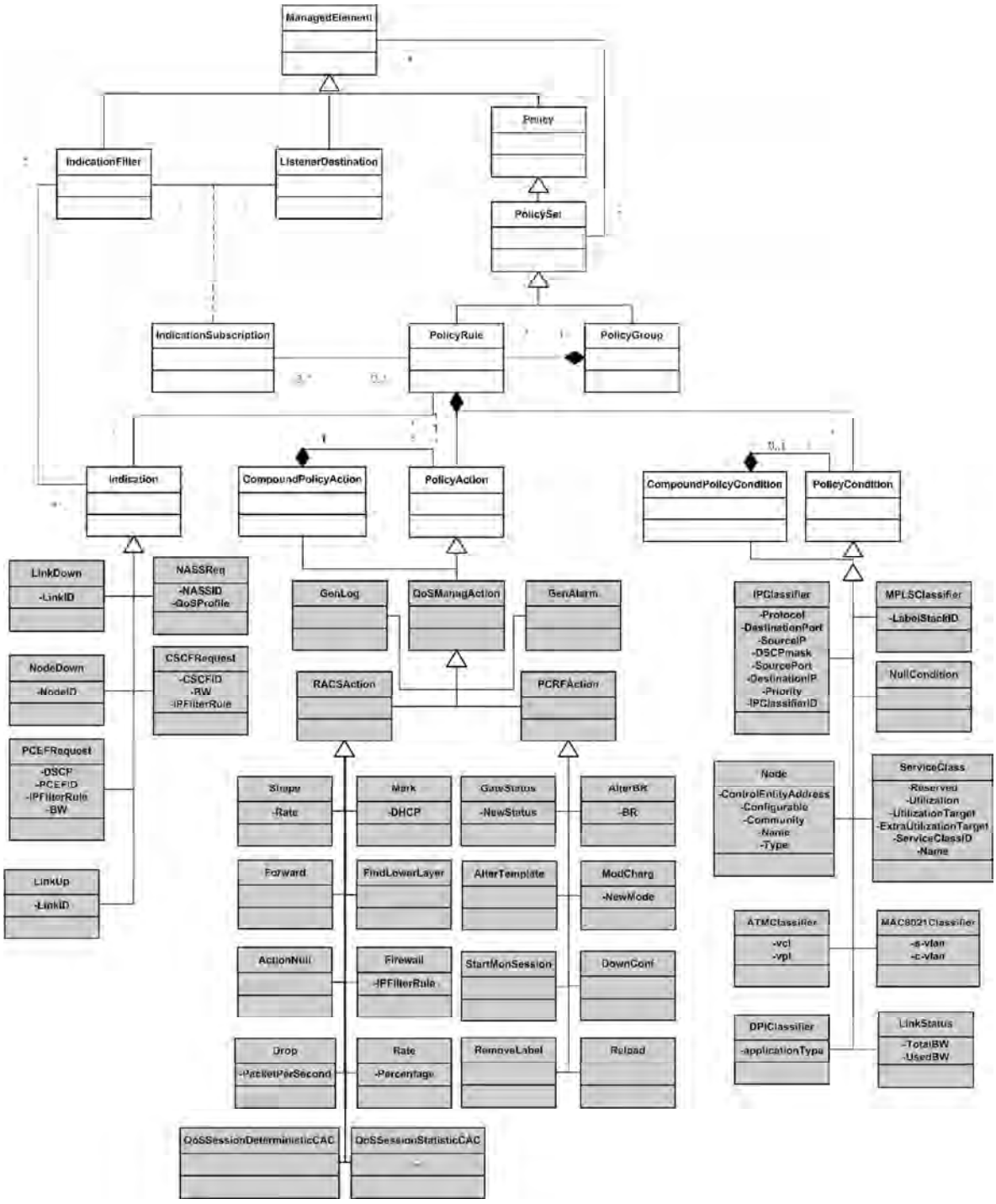

Figura 10.1 - Modelo de dados de políticas completo.

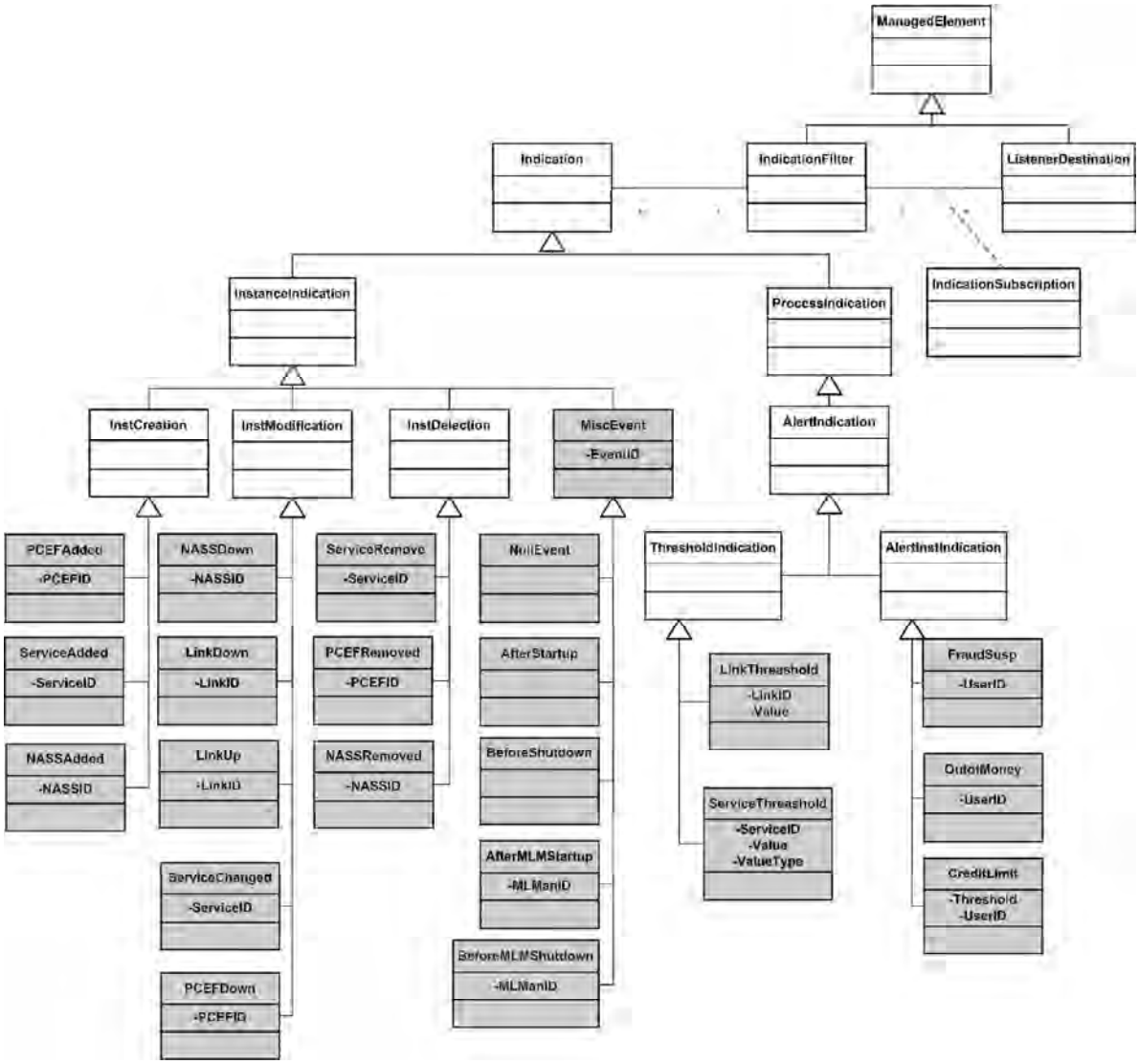

Figura 10.2 - Modelos de dados de eventos.

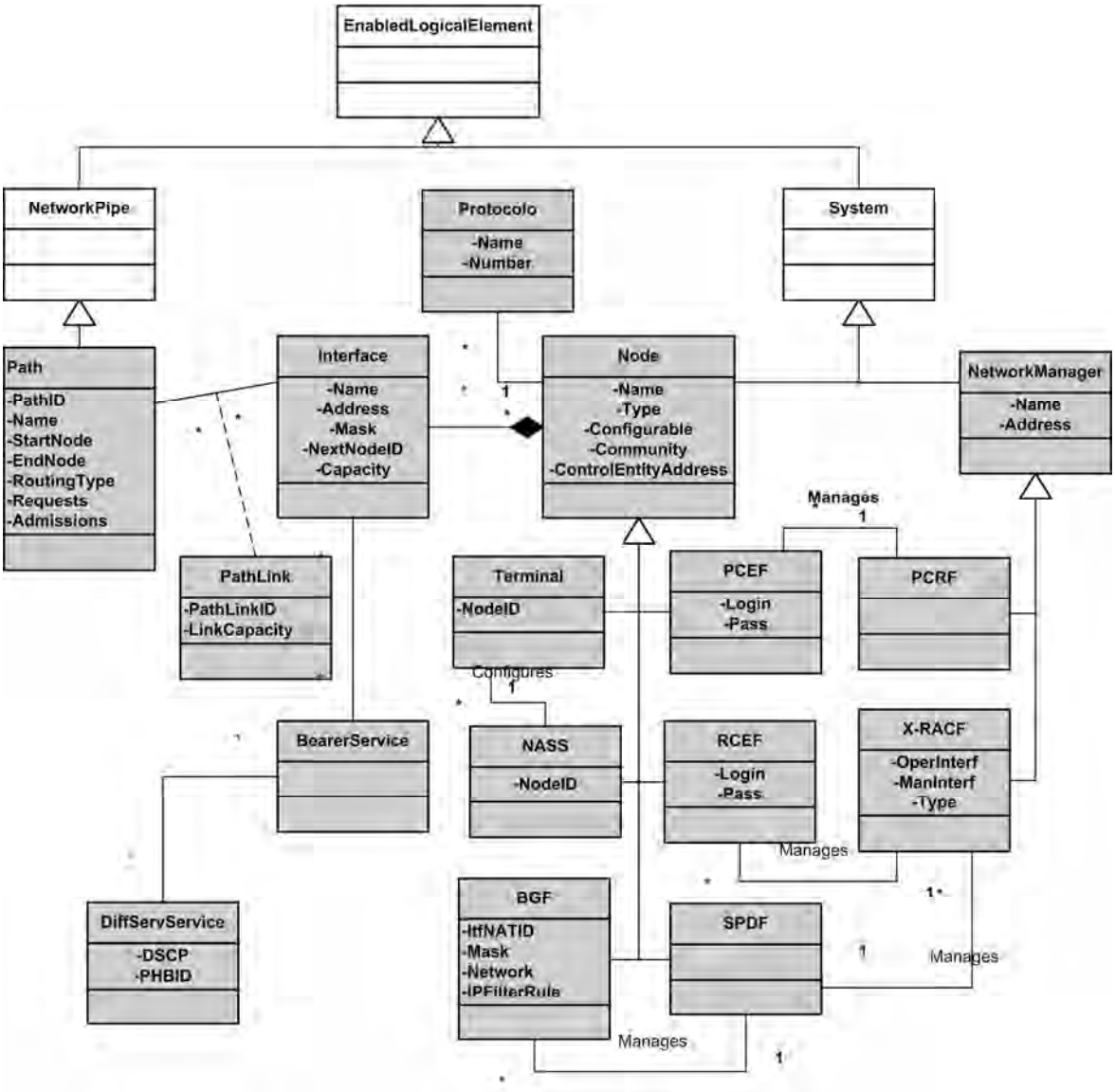

Figura 10.3 - Modelo de dados de recursos.

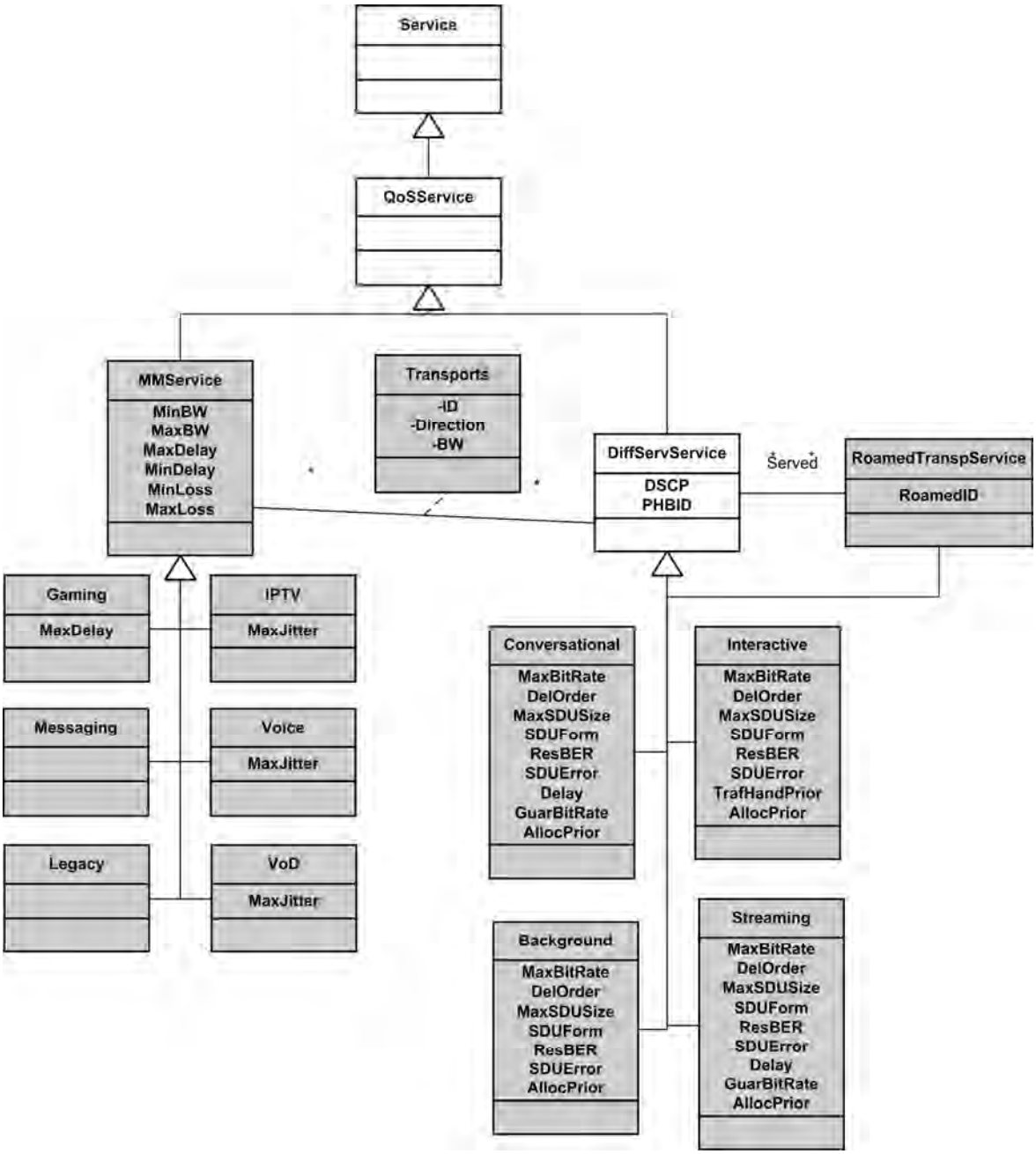

Figura 10.4 - Modelo de dados dos serviços.